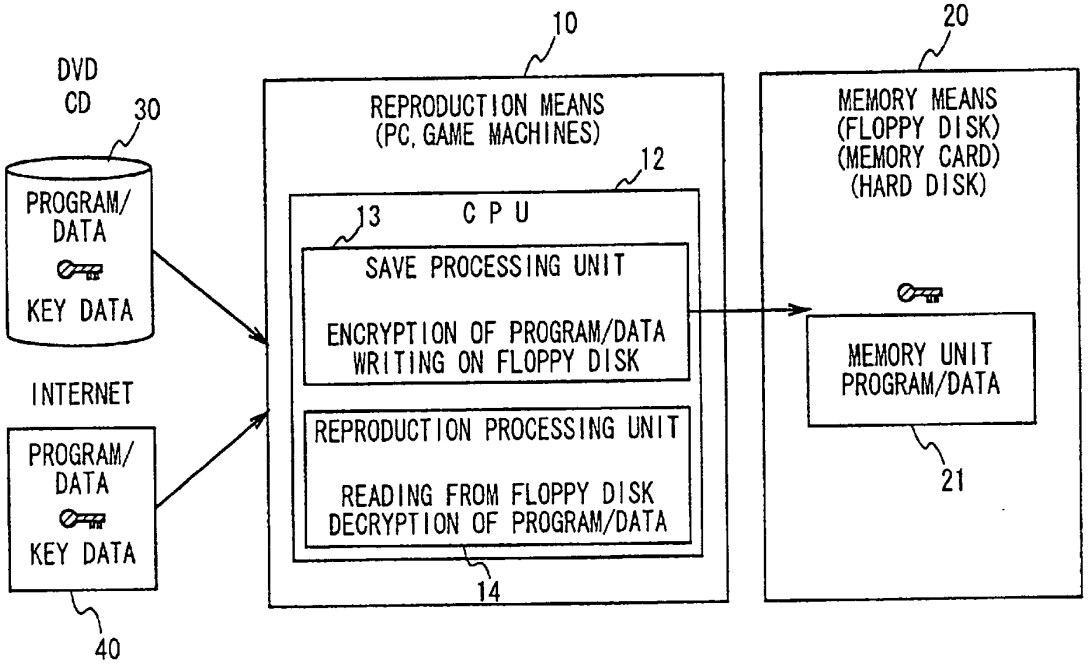


FIG. 1

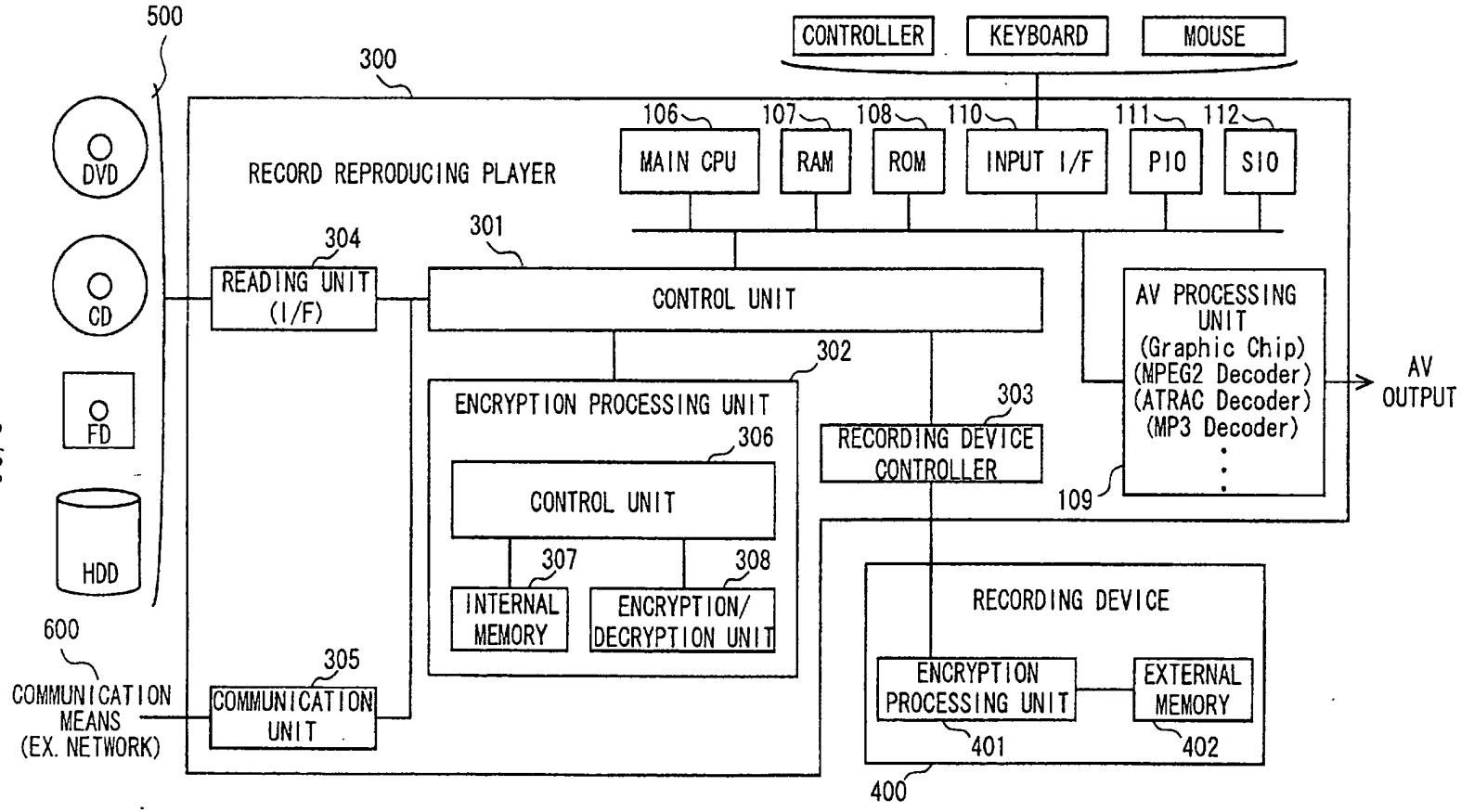

500
300
CONTROLLER
KEYBOARD
MOUSE
DVD
CD
FD
HDD
RECORD REPRODUCING PLAYER
106
MAIN CPU
107
RAM
108
ROM
110
INPUT I/F
111
PIO
112
SIO
304
READING UNIT (I/F)
301
CONTROL UNIT
AV PROCESSING UNIT (Graphic Chip) (MPEG2 Decoder) (ATRAC Decoder) (MP3 Decoder)
AV OUTPUT
302
ENCRYPTION PROCESSING UNIT
303
RECORDING DEVICE CONTROLLER
306
CONTROL UNIT
307
INTERNAL MEMORY
308
ENCRYPTION/ DECRYPTION UNIT
109
RECORDING DEVICE
ENCRYPTION PROCESSING UNIT
401
EXTERNAL MEMORY
402
400
600
COMMUNICATION MEANS (EX. NETWORK)
305
COMMUNICATION UNIT

FIG. 2

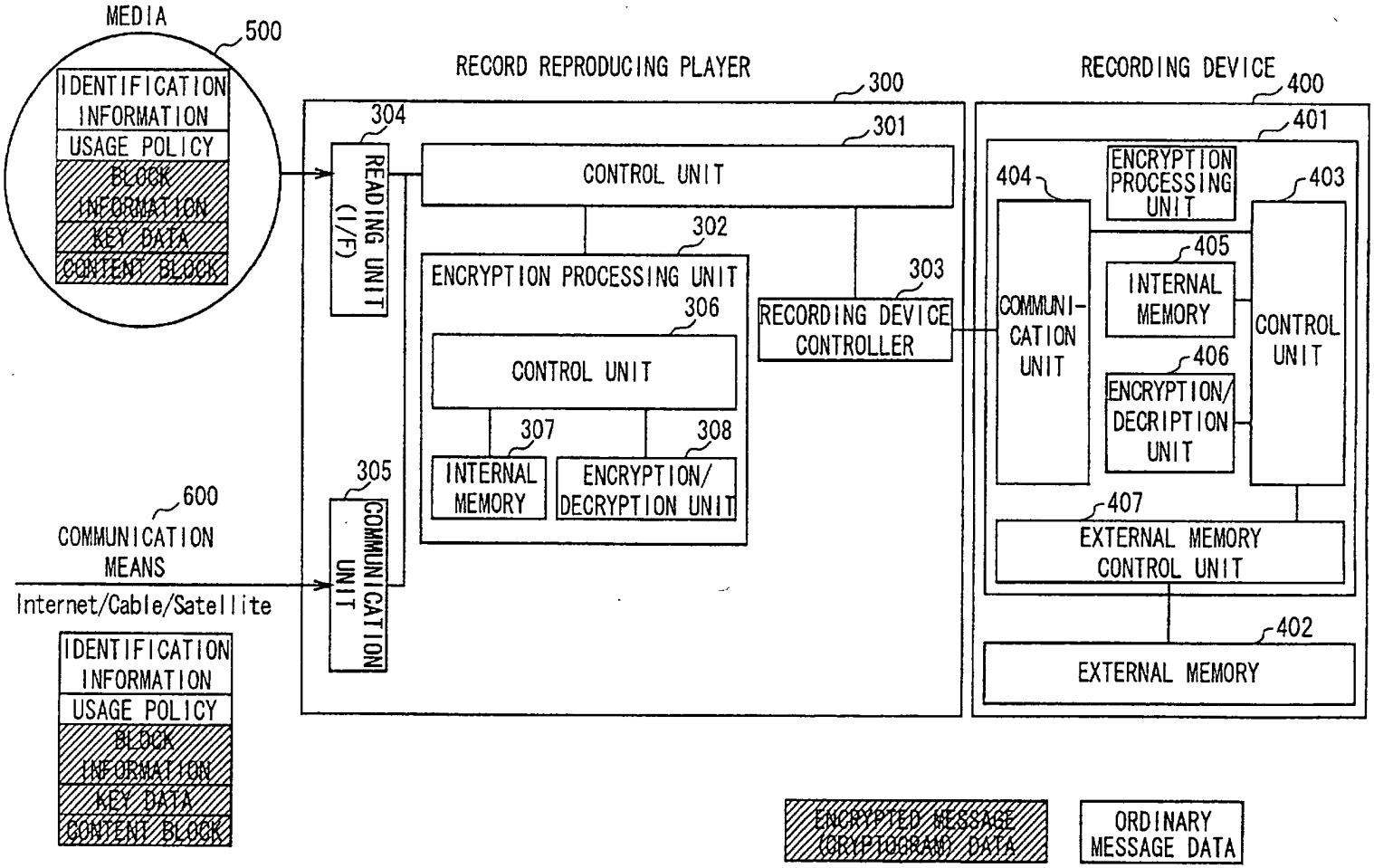


FIG. 3

DATA FORMAT ON MEDIA & COMMUNICATIONS ROUTE

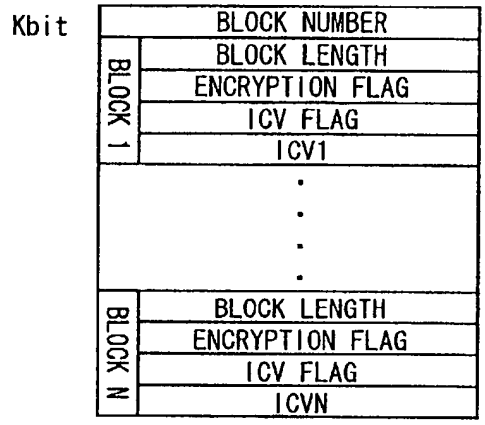
FIG. 4

09/937410

HEADER LENGTH
CONTENT LENGTH
FORMAT VERSION
FORMAT TYPE
CONTENT TYPE
OPERATION PRIORITY
LOCALIZATION FIELD
COPY PERMISSION
MOVE PERMISSION
ENCRYPTION ALGORITHM
ENCRYPTION MODE
INTEGRITY CHECK METHOD

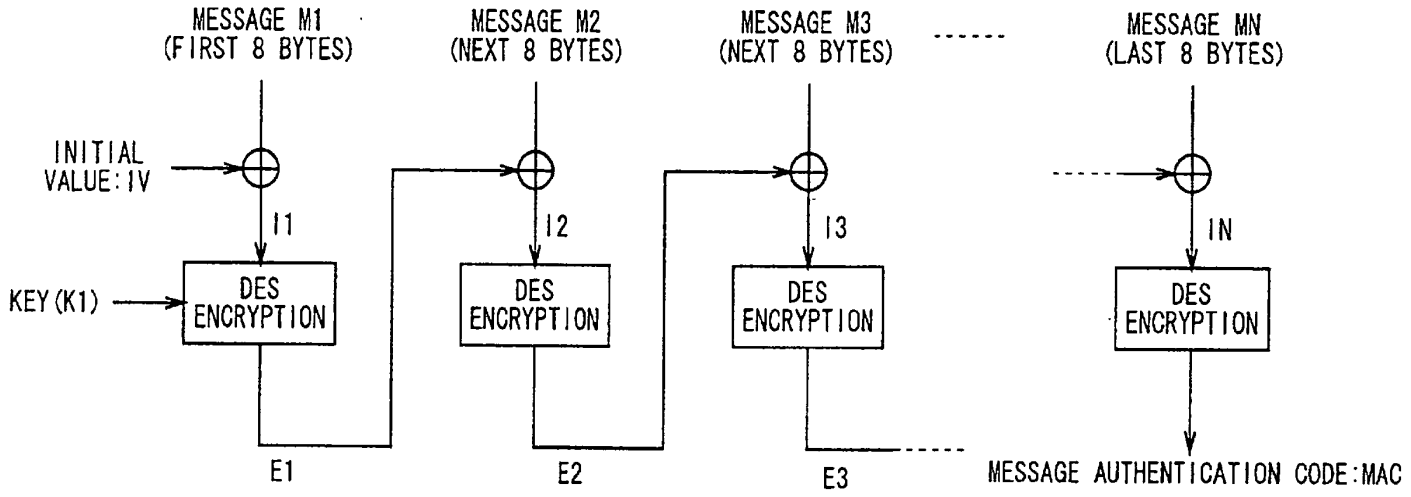
USAGE POLICY

FIG. 5



BLOCK INFORMATION

FIG. 6



⊕:EXCLUSIVE OR (XOR) PROCESS (8-BYTE UNIT)

FIG. 7

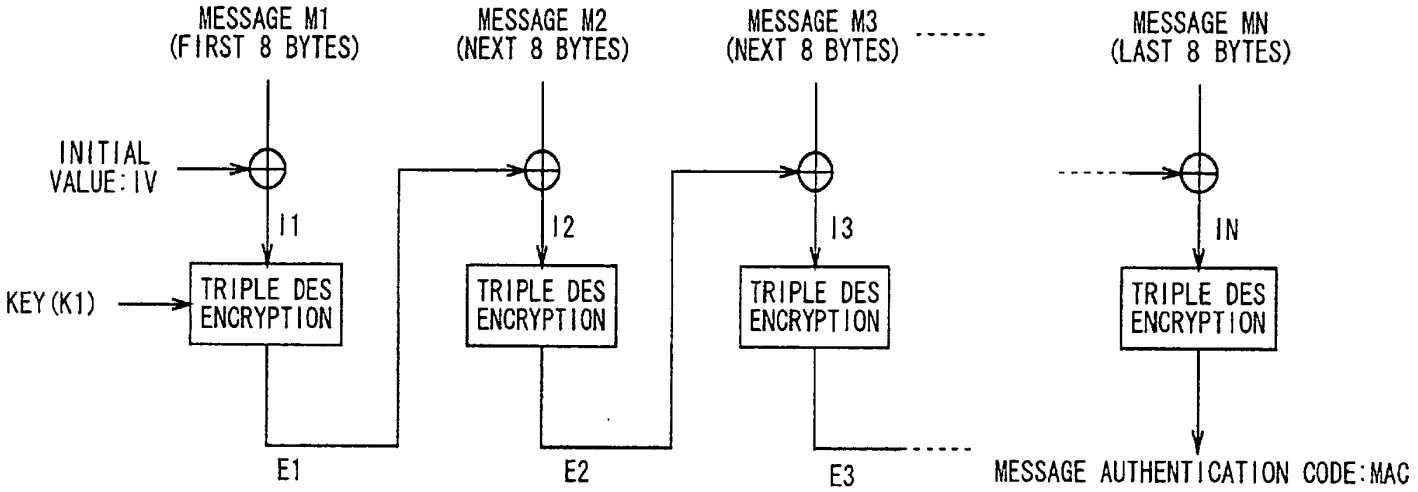
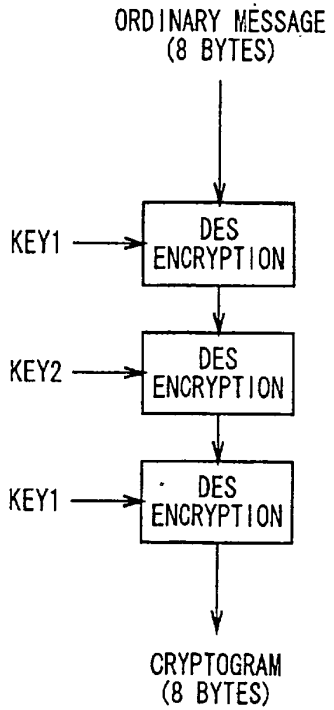
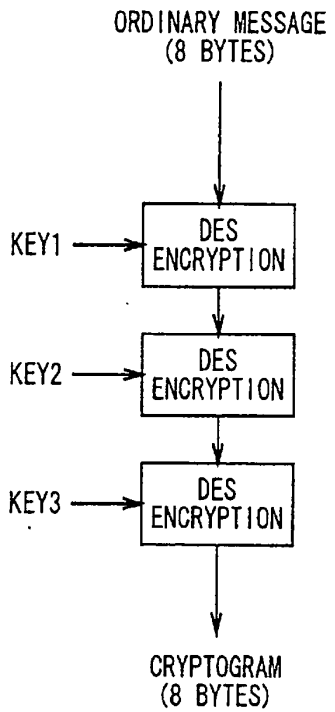


FIG. 8


ORDINARY MESSAGE
(8 BYTES)
KEY1
DES
ENCRYPTION
KEY2
DES
ENCRYPTION
KEY1
DES
ENCRYPTION
CRYPTOGRAM
(8 BYTES)

(A)


ORDINARY MESSAGE
(8 BYTES)
KEY1
DES
ENCRYPTION
KEY2
DES
ENCRYPTION
KEY3
DES
ENCRYPTION
CRYPTOGRAM
(8 BYTES)

(B)

FIG. 9

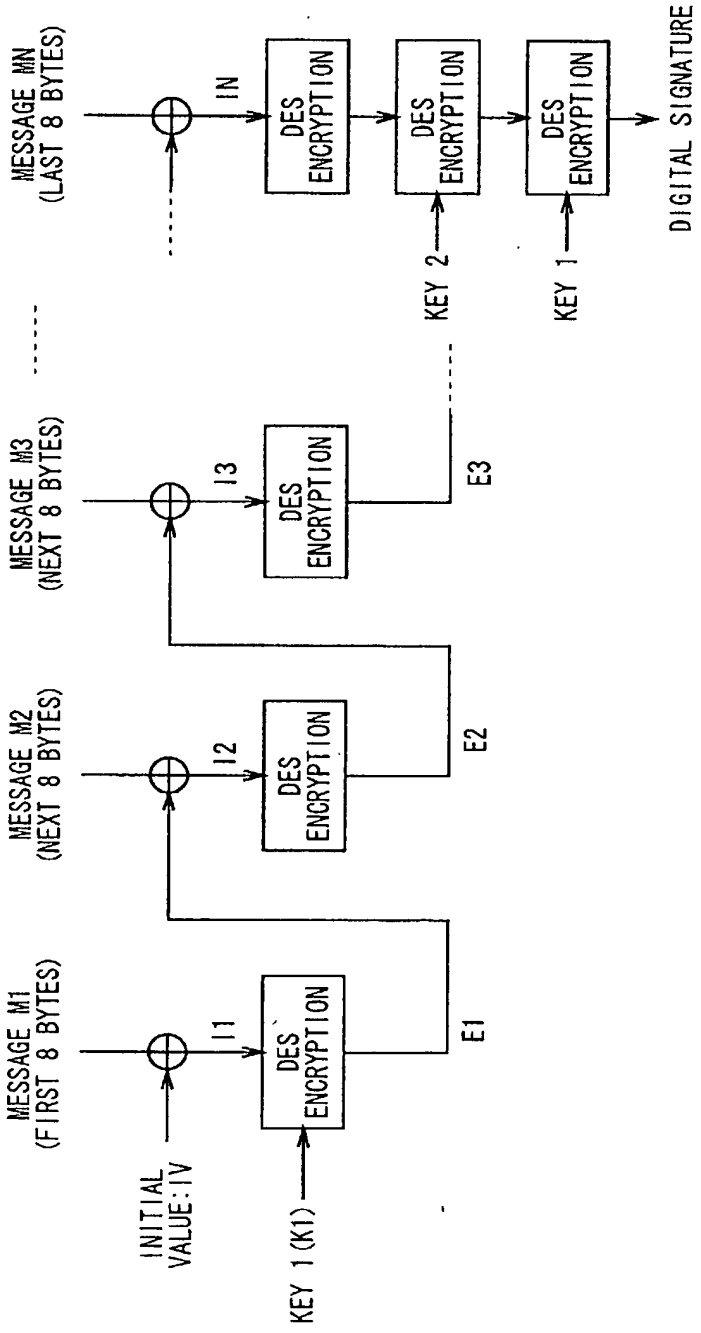
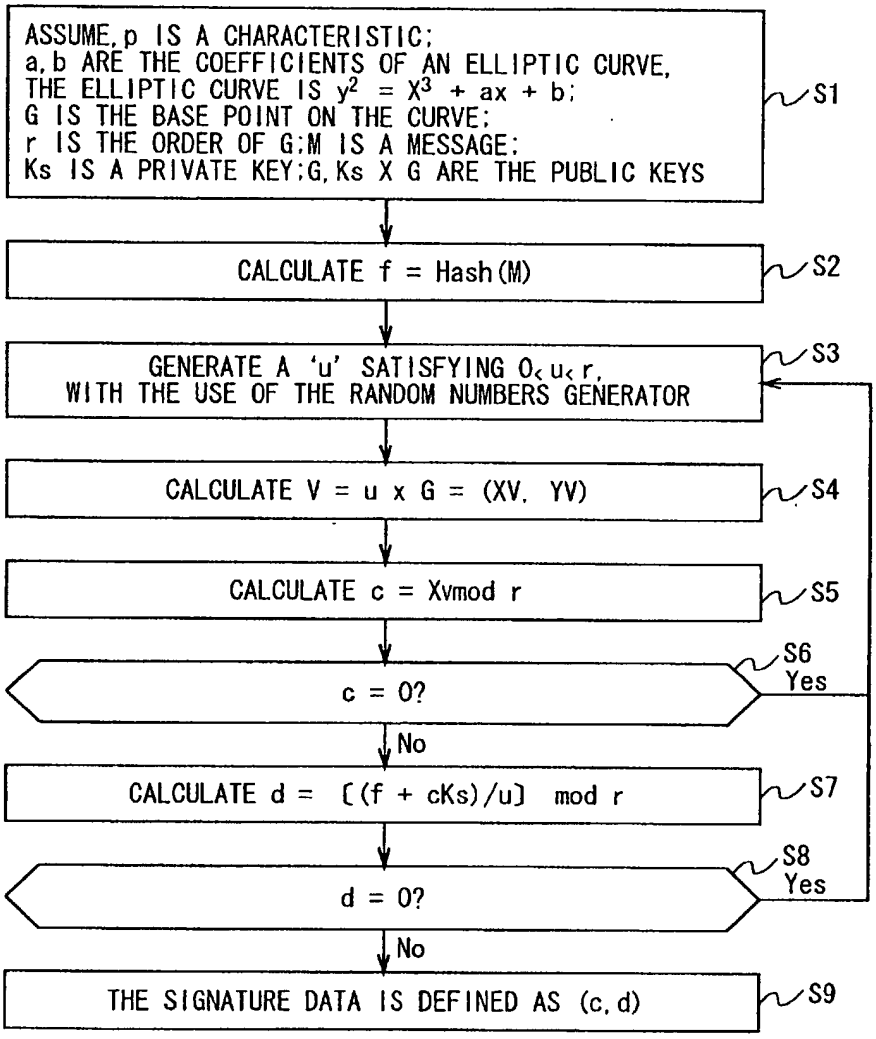

MESSAGE M1
(FIRST 8 BYTES)
MESSAGE M2
(NEXT 8 BYTES)
MESSAGE M3
(NEXT 8 BYTES)
MESSAGE MN
(LAST 8 BYTES)
INITIAL
VALUE:IV
KEY 1 (K1)
I1
I2
I3
IN
DES
ENCRYPTION
E1
E2
E3
KEY 2
KEY 1
DIGITAL SIGNATURE

FIG. 10

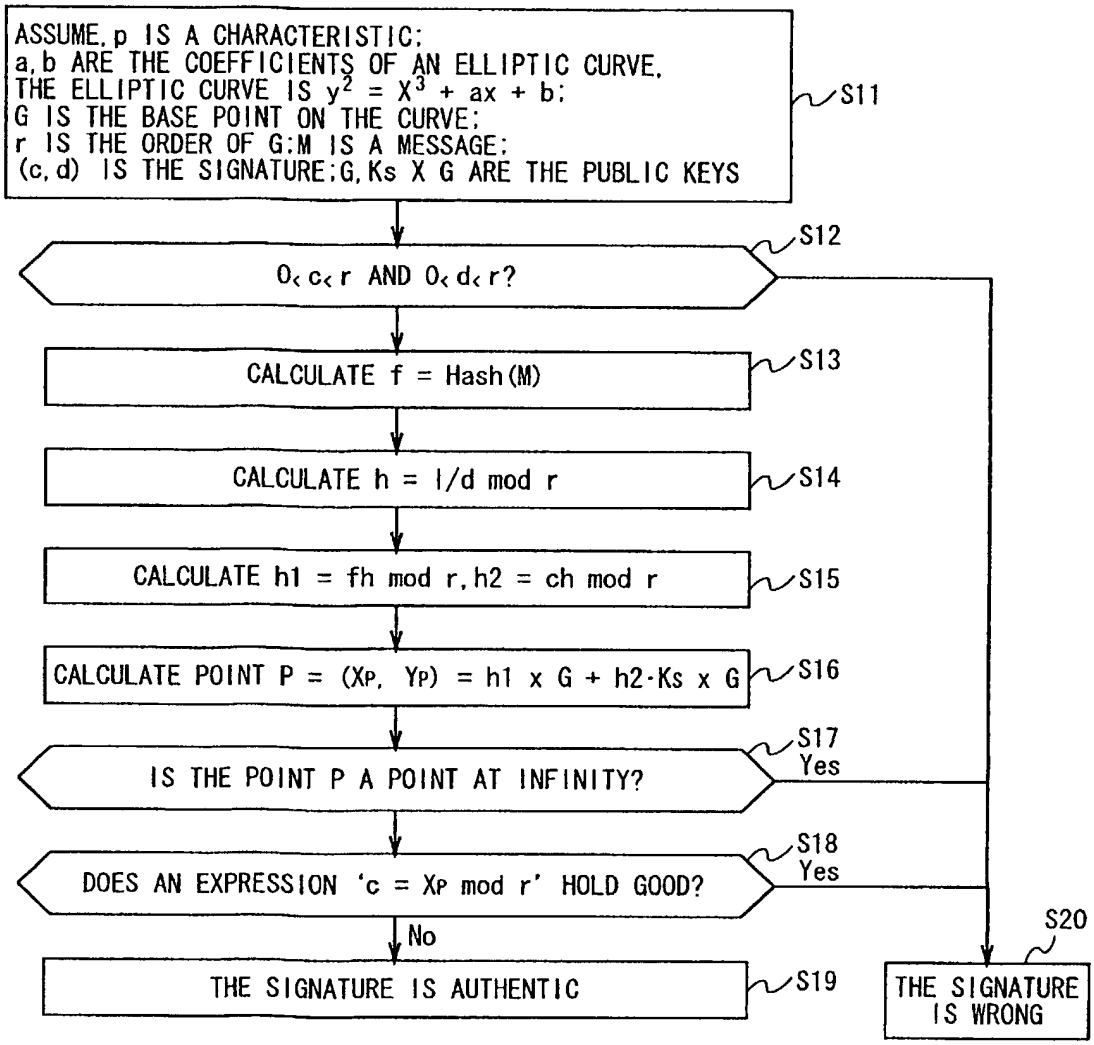
GENERATION OF SIGNATURE



GENERATION OF SIGNATURE (IEEE P1363/D3)

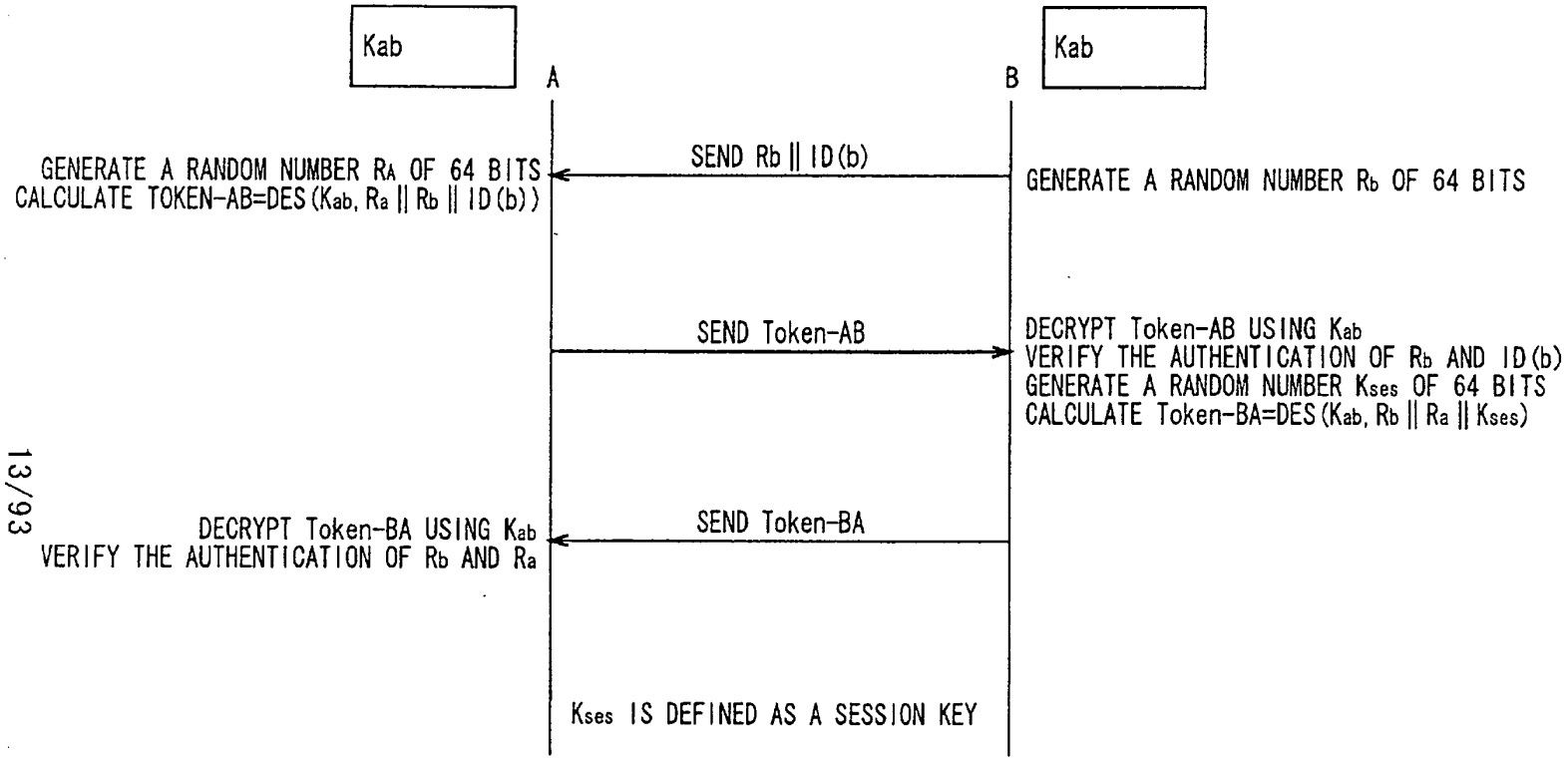
FIG. 11

AUTHENTICATION OF SIGNATURE



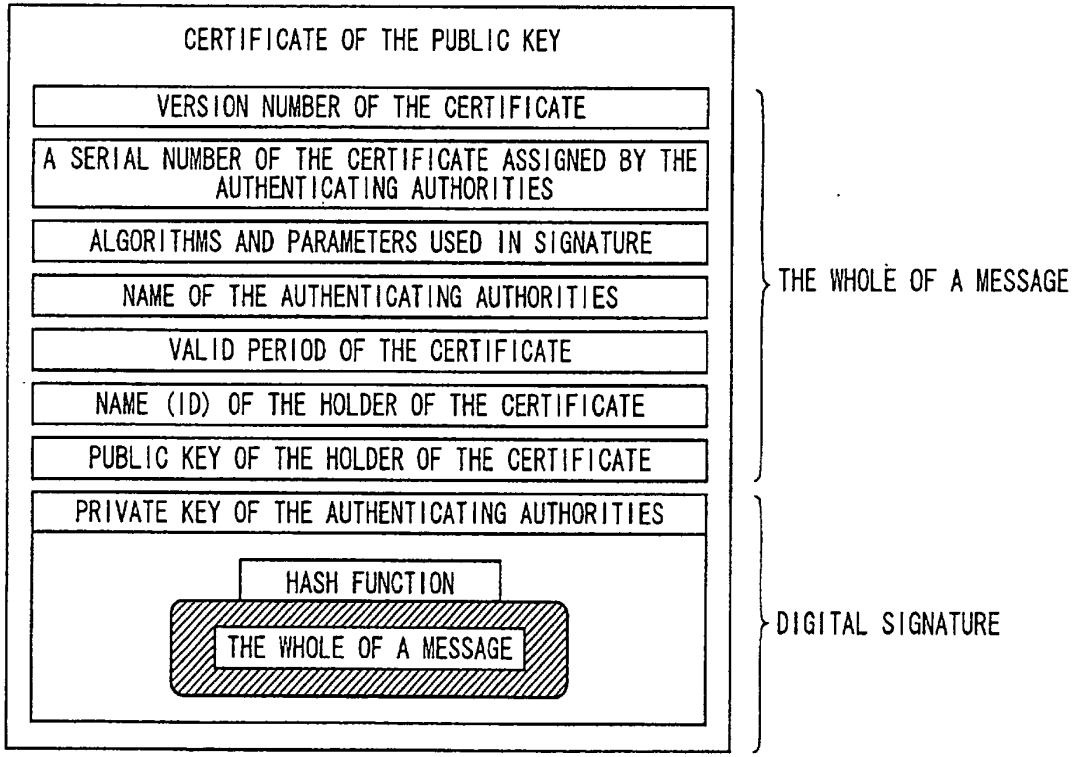
AUTHENTICATION OF SIGNATURE (IEEE P1363/D3)

FIG. 12



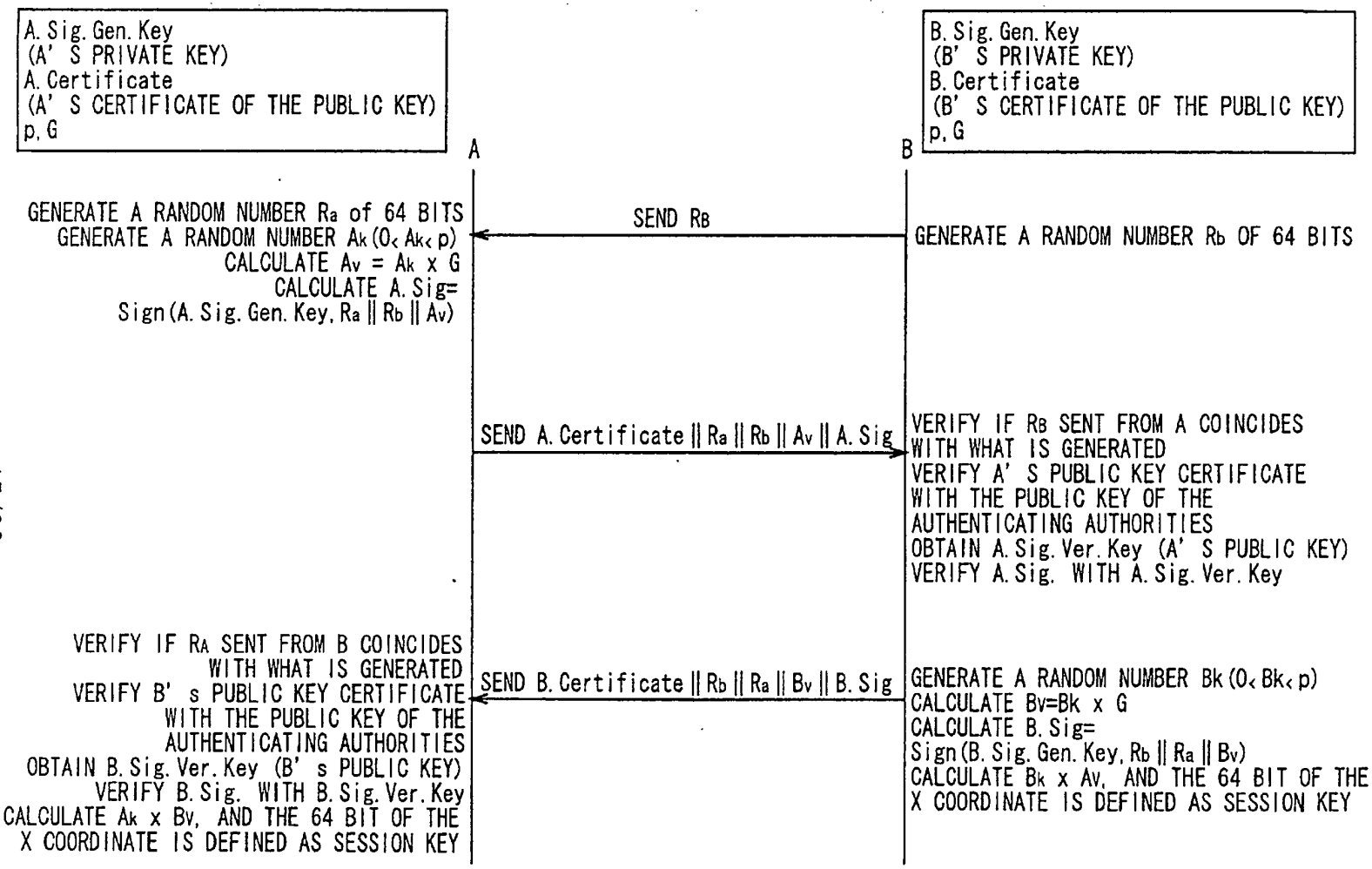
ISO/IEC 9798-2 MUTUAL AUTHENTICATION AND SHARED KEY DEVICE USING SYMMETRIC ENCIPHERMENT ALGORITHMS (SYMMETRIC KEY ENCRIPTION TECHNOLOGY

FIG. 13



CERTIFICATE OF PUBLIC KEY

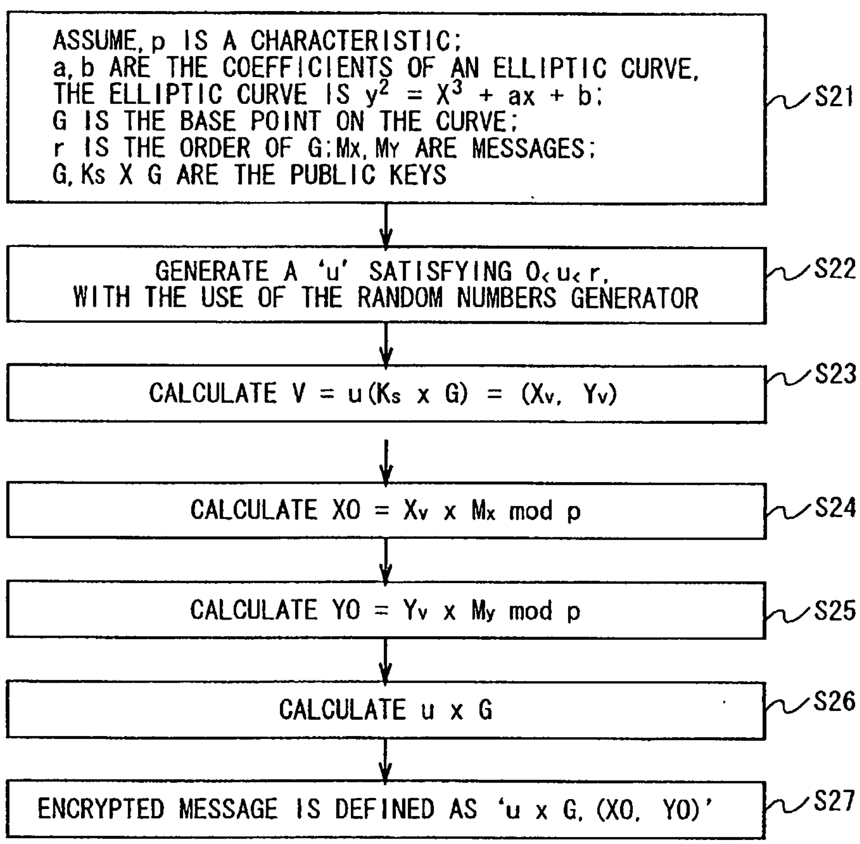
FIG. 14



ISO/IEC 9798-3 MUTUAL AUTHENTICATION AND SHARED KEY SYSTEM USING SYMMETRIC ENCIPHERMENT ALGORITHMS (SYMMETRIC KEY ENCRYPTION TECHNOLOGY)

FIG. 15

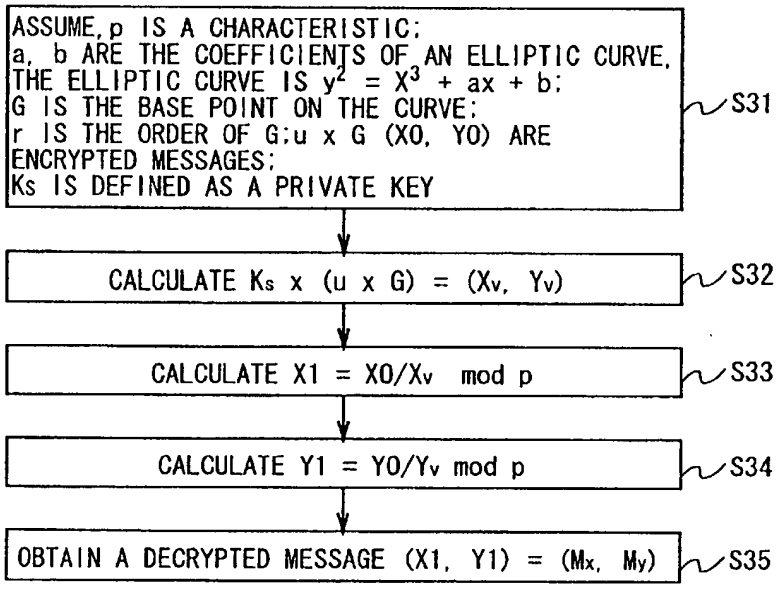
ENCYPTION



ENCRYPTION USING ELLIPTIC CURVE ENCRYPTION METHOD (MENEZES-VANSTONE)

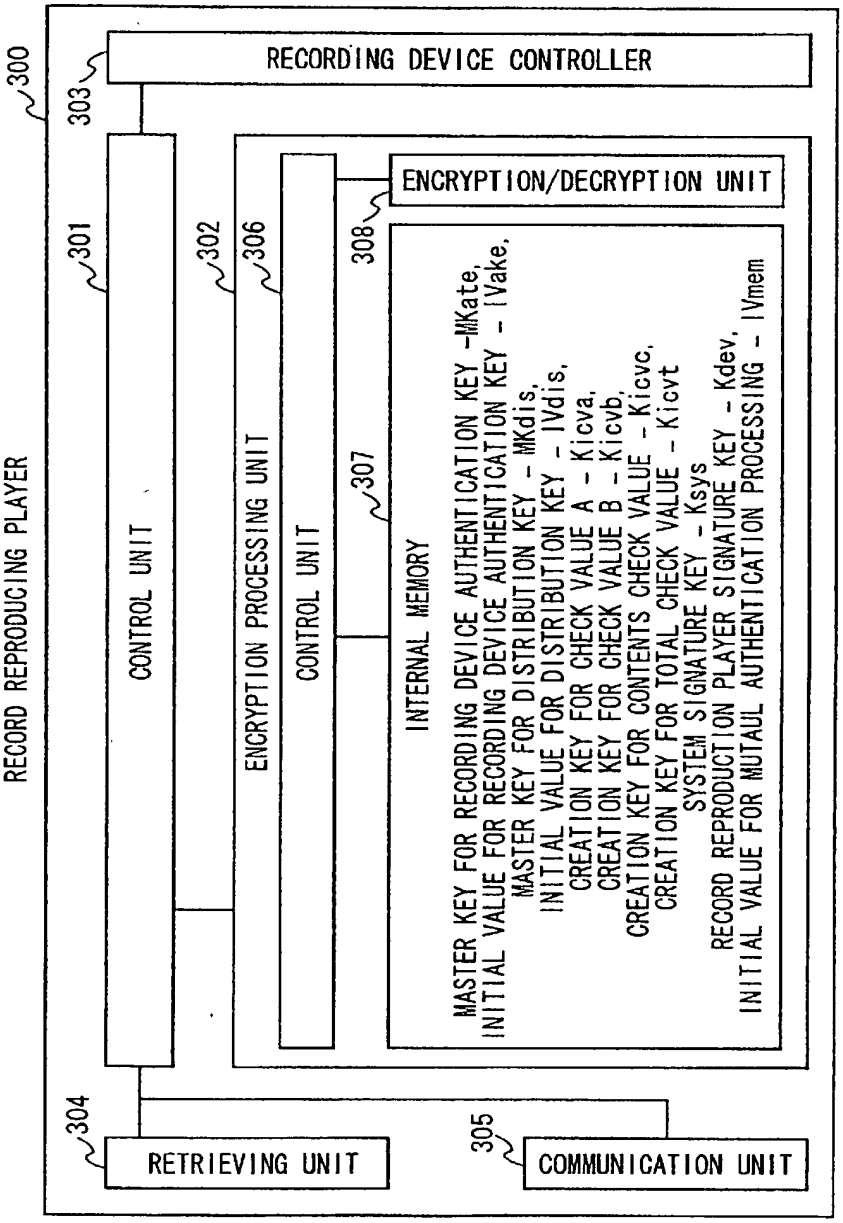
FIG. 16

DECRYPTION



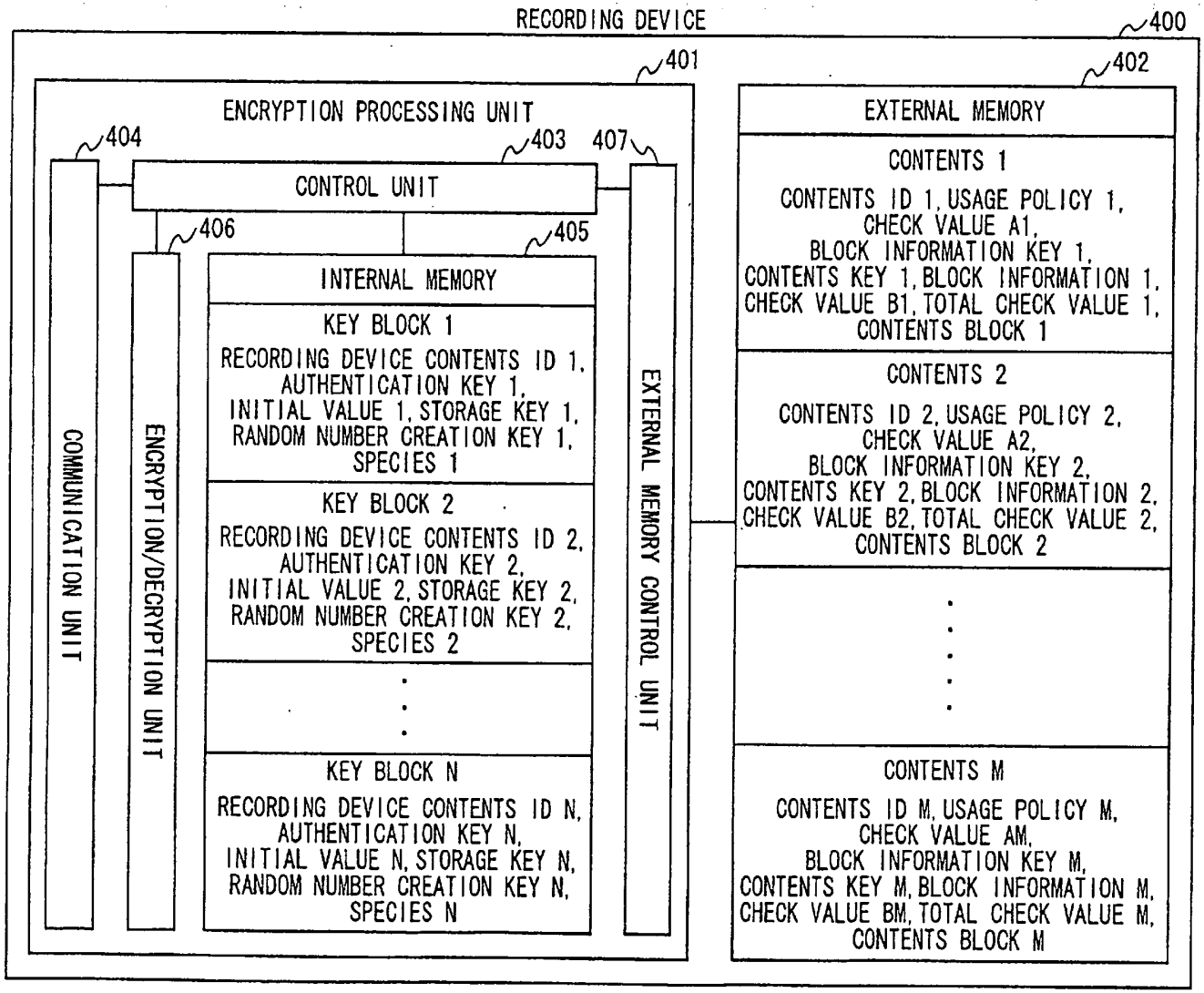
DECRYPTION USING ELLIPTIC CURVE ENCRYPTION MTHOD (MENEZES-VANSTONE)

FIG. 17



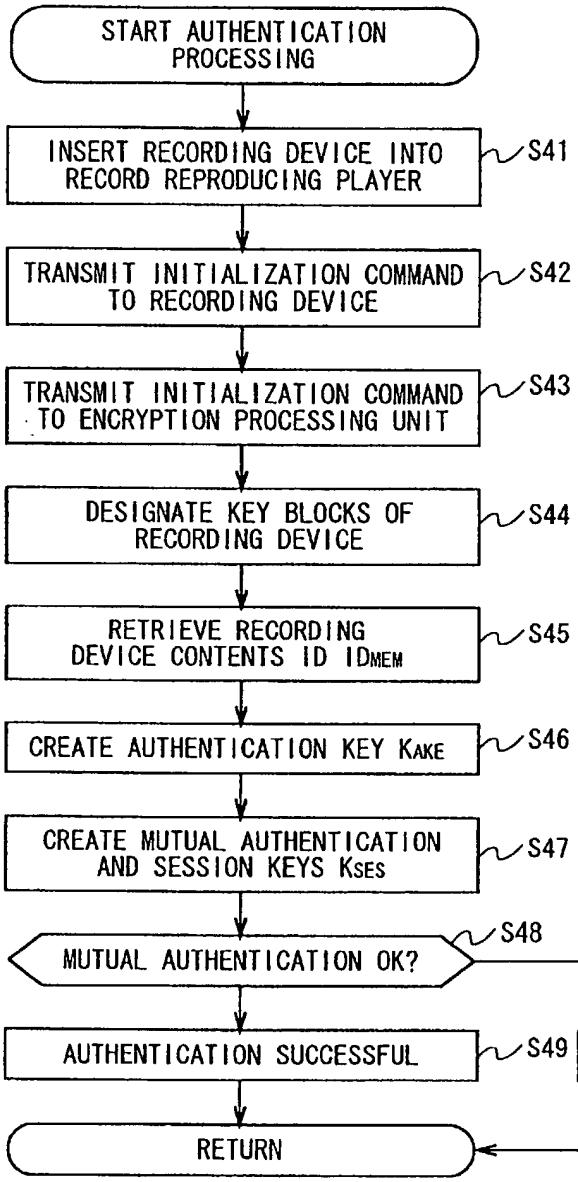
DATA RETAINING STATE ON RECORD REPRODUCING PLAYER

FIG.18



DATA RETAINING STATE ON RECORDING DEVICE

FIG. 19



MUTUAL AUTHENTICATION BETWEEN RECORD REPRODUCTION AND RECORDING DEVICE

FIG. 20

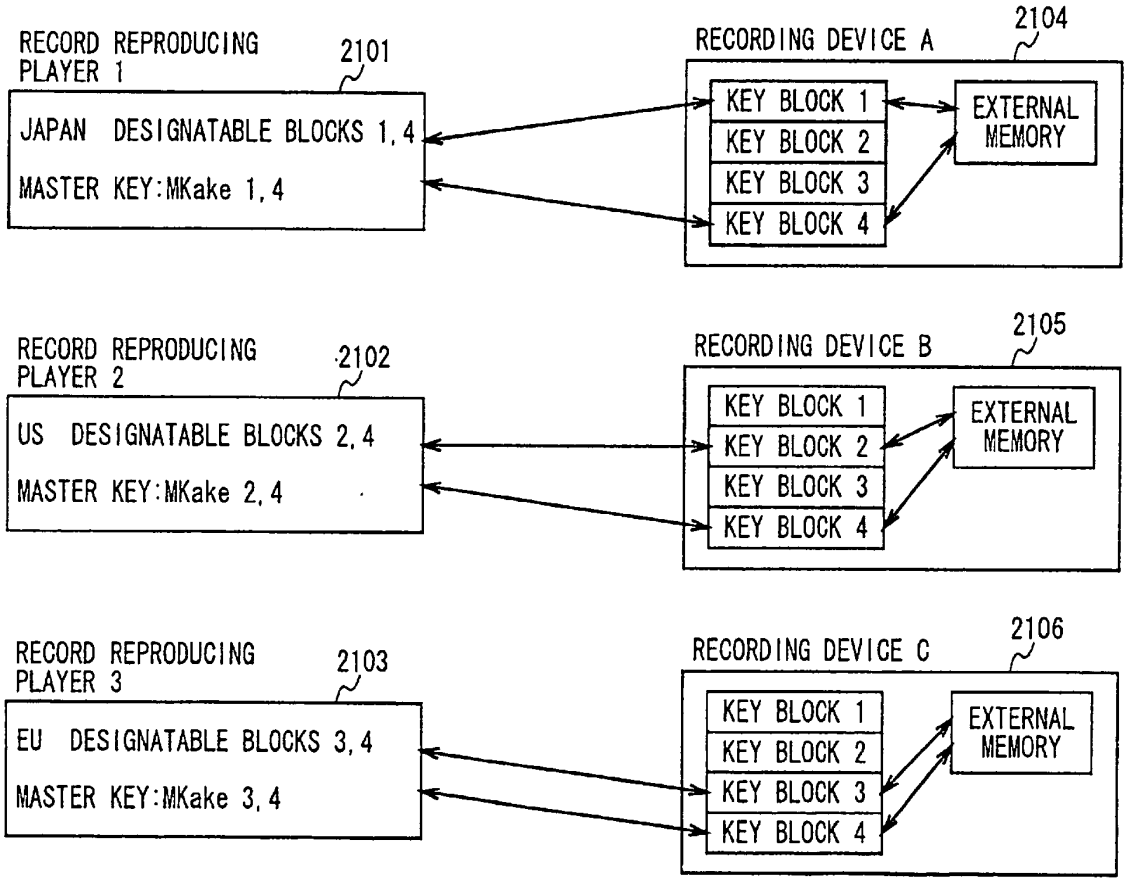
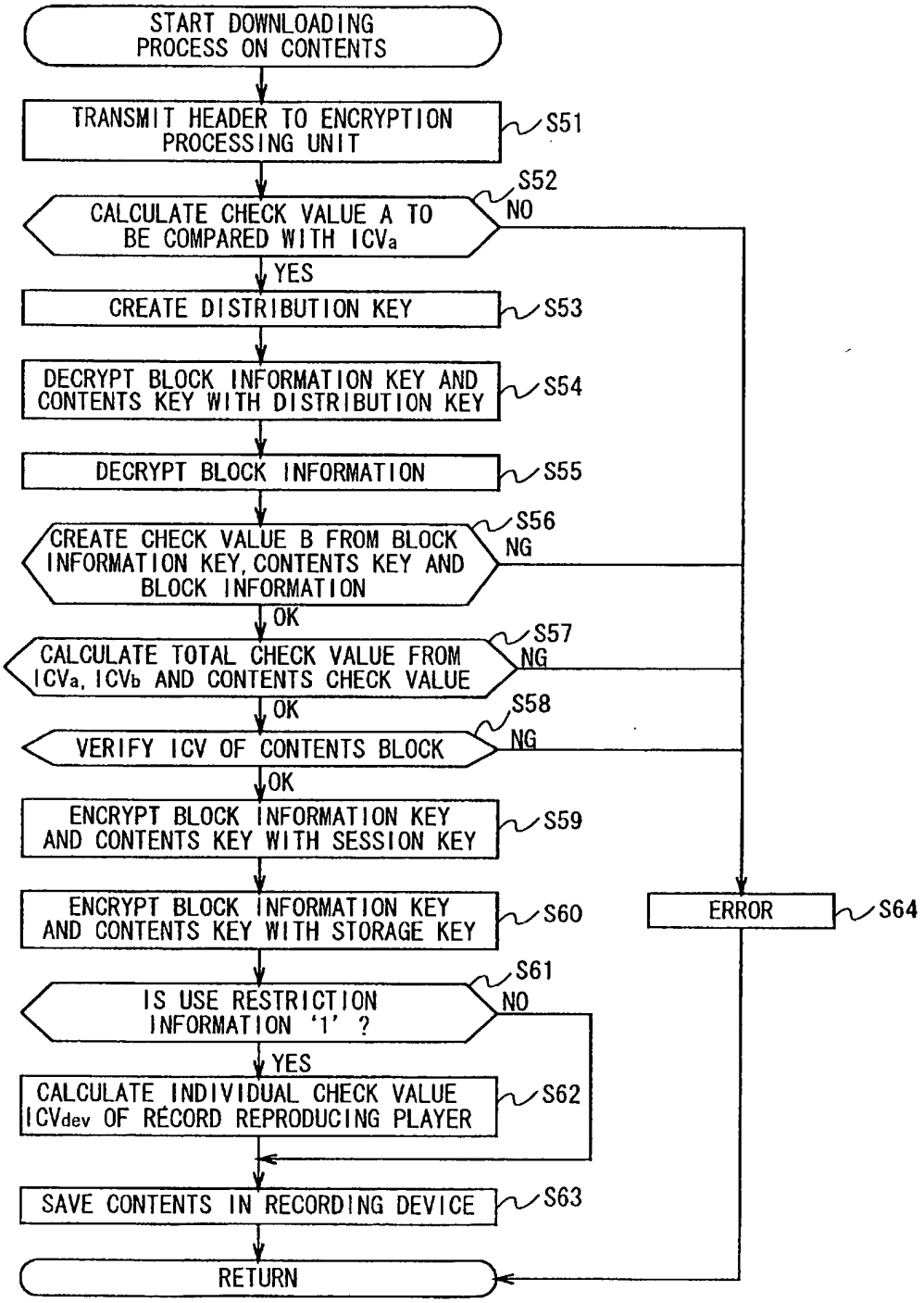
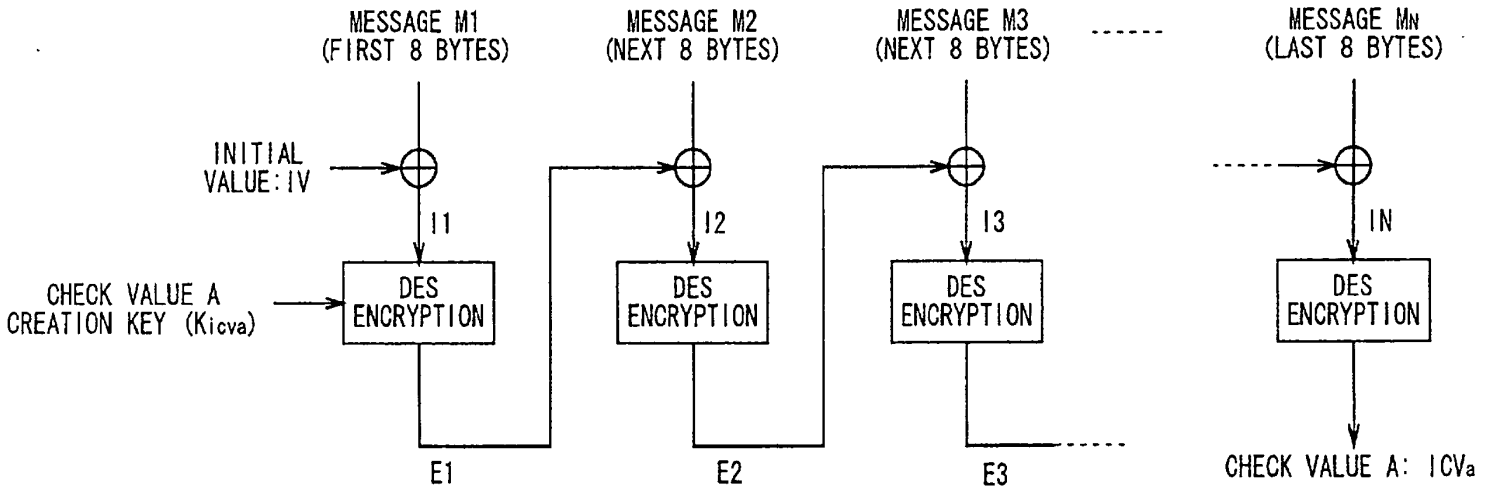


FIG. 21



DOWNLOADING PROCESS OF CONTENTS

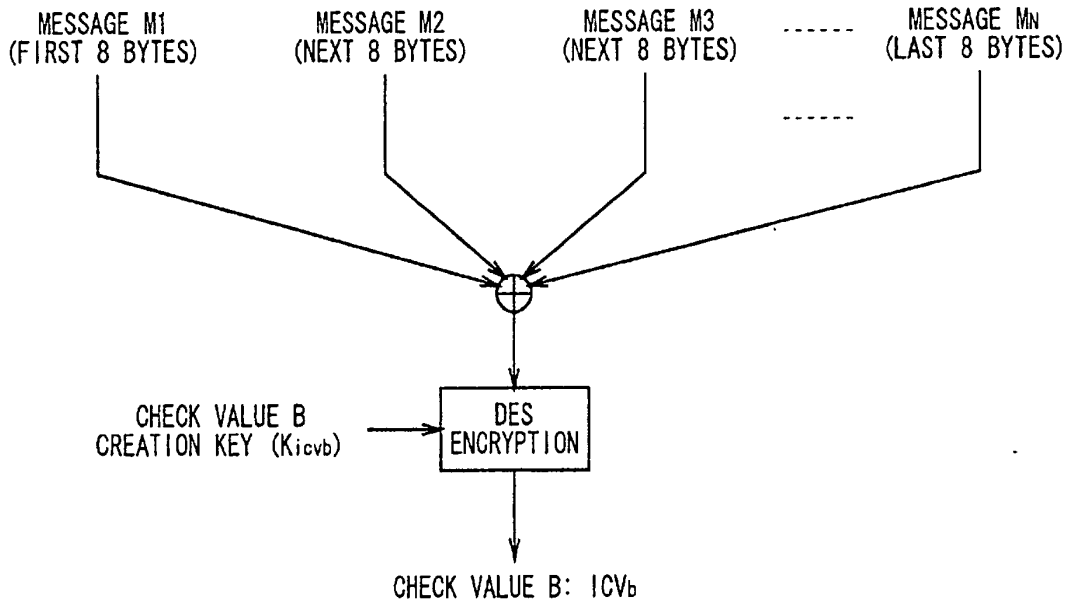
FIG. 22



MESSAGE M1 - MN: CONTENTS ID, USAGE POLICY

⊕:EXCLUSIVE OR (XOR) PROCESS (8-BYTE UNIT)

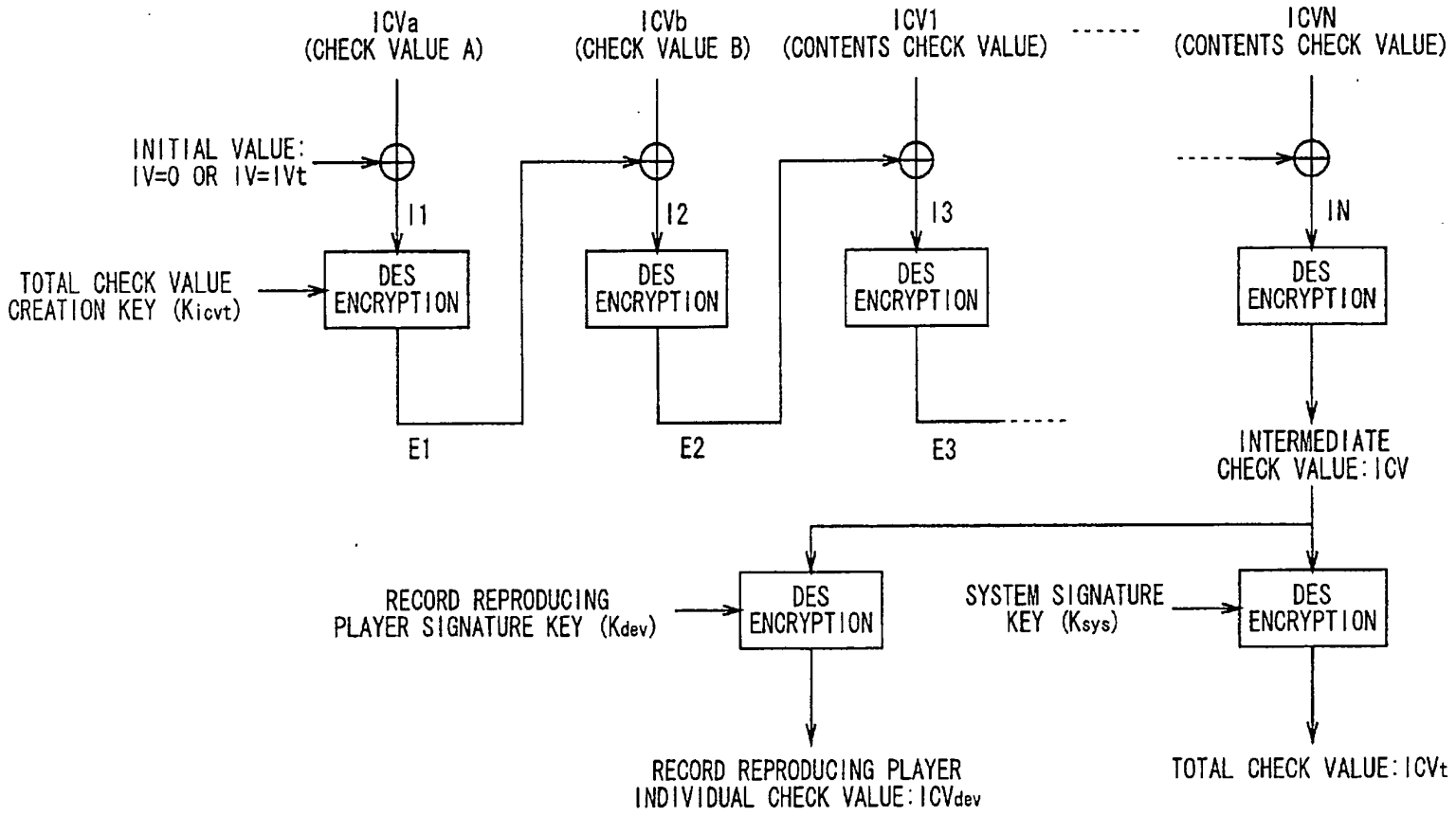
FIG. 23



MESSAGE M1 - MN: BLOCK INFORMATION KEY Kbit, CONTENTS KEY Kcon, BLOCK INFORMATION

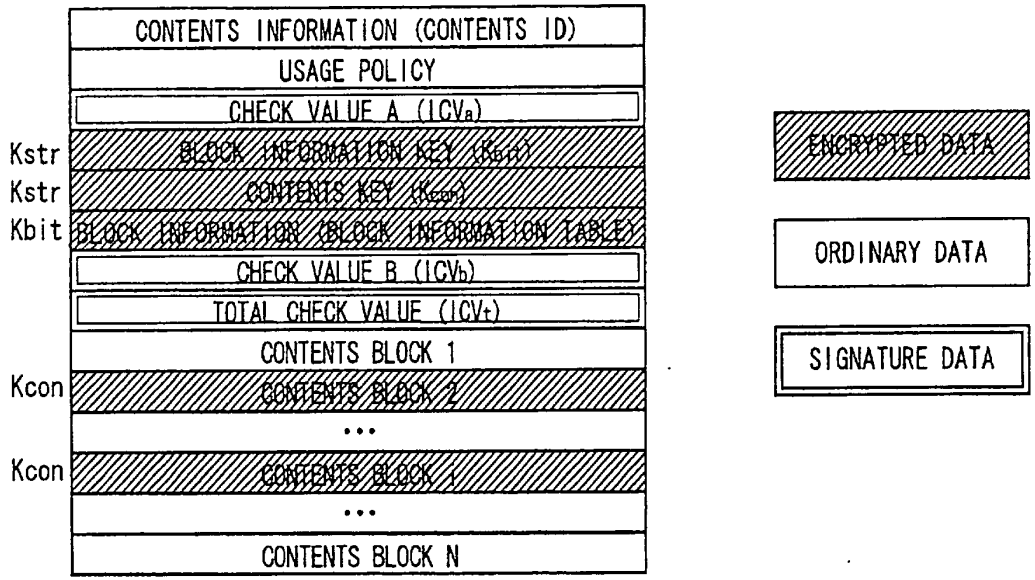
⊕:EXCLUSIVE OR (XOR) PROCESS (8-BYTE UNIT)

FIG. 24



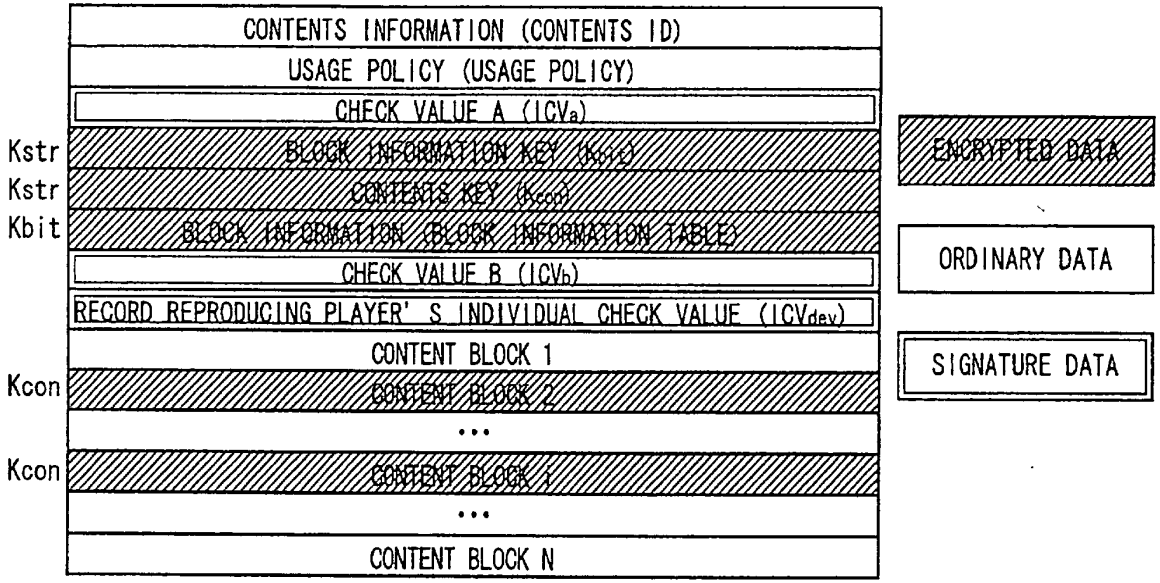
⊕:EXCLUSIVE OR (XOR) PROCESS (8-BYTE UNIT)

FIG. 25



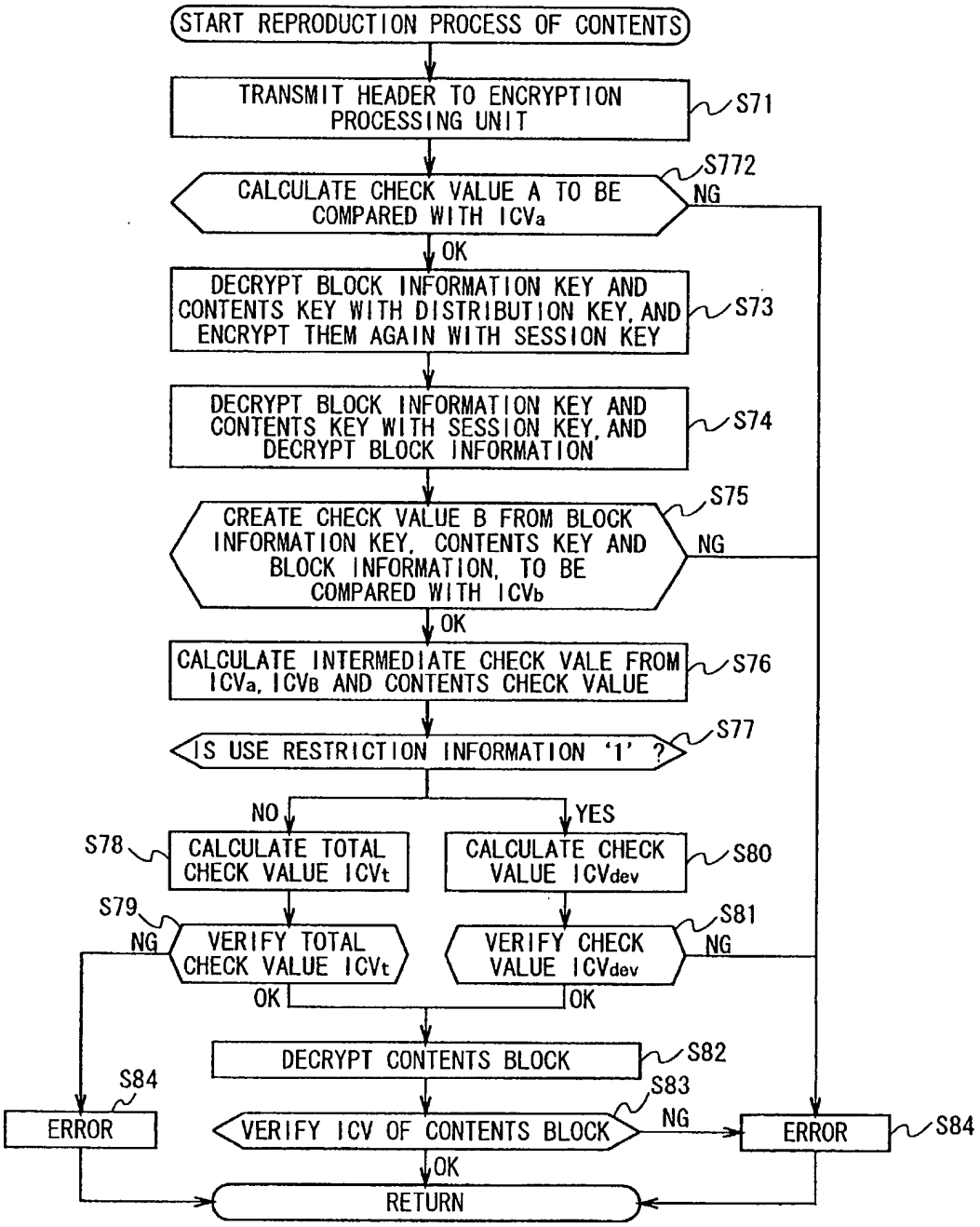
CONTENTS SAVED IN RECORDING DEVICE
(USE RESTRICTION INFORMATION = 0)

FIG. 26



CONTENTS SAVED IN RECORDING DEVICE
(USE RESTRICTION INFORMATION = 1)

FIG. 27



REPRODUCTION PROCESS OF CONTENTS

FIG. 28

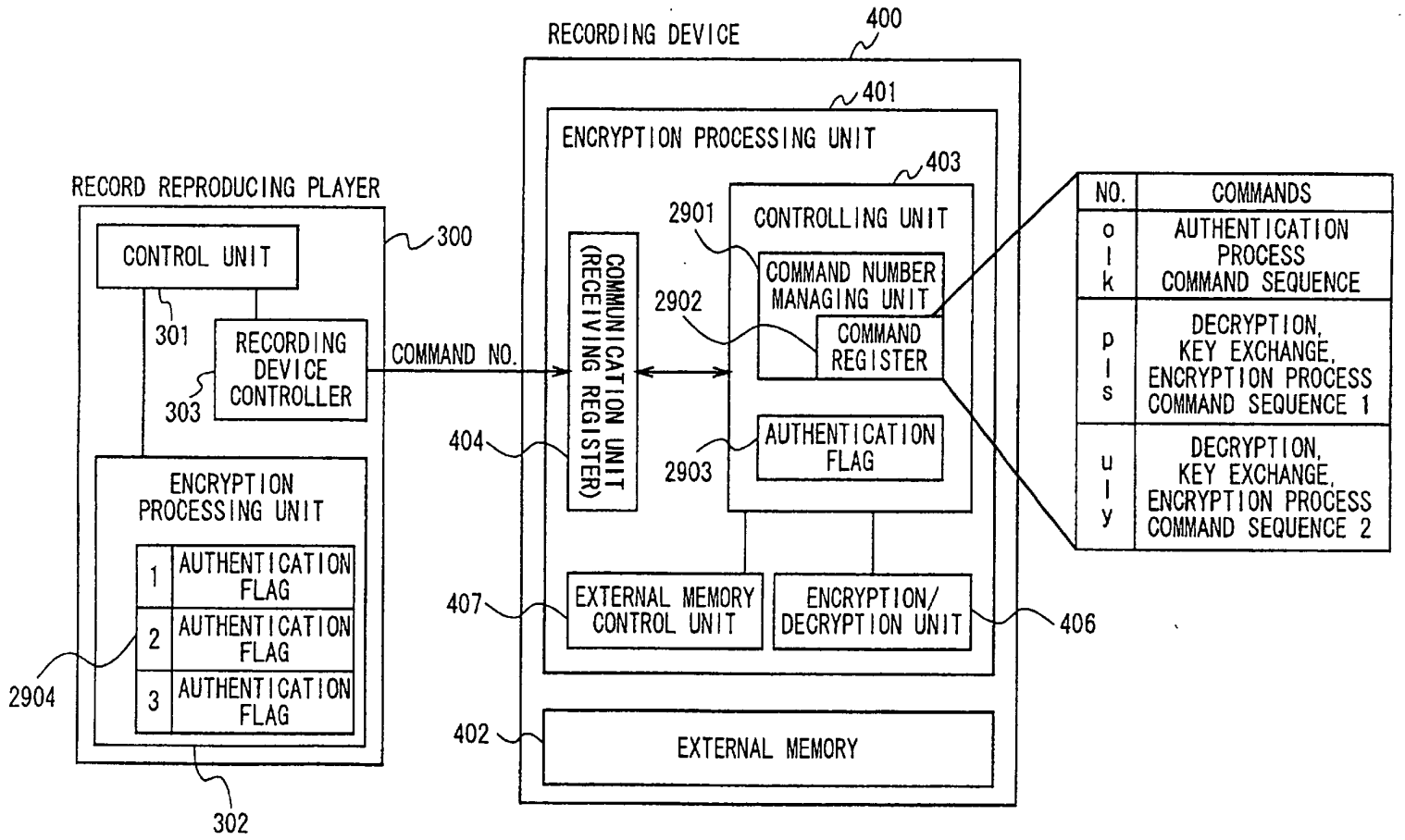


FIG. 29

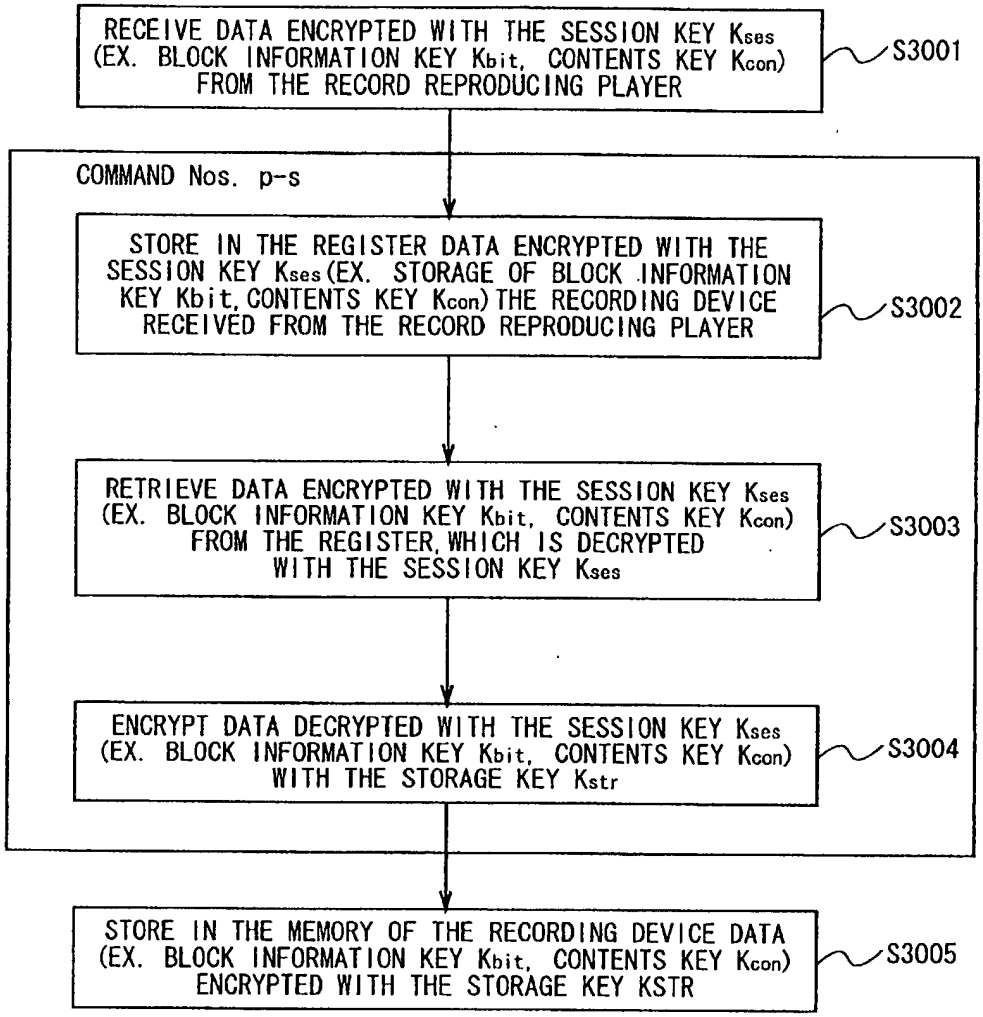


FIG. 30

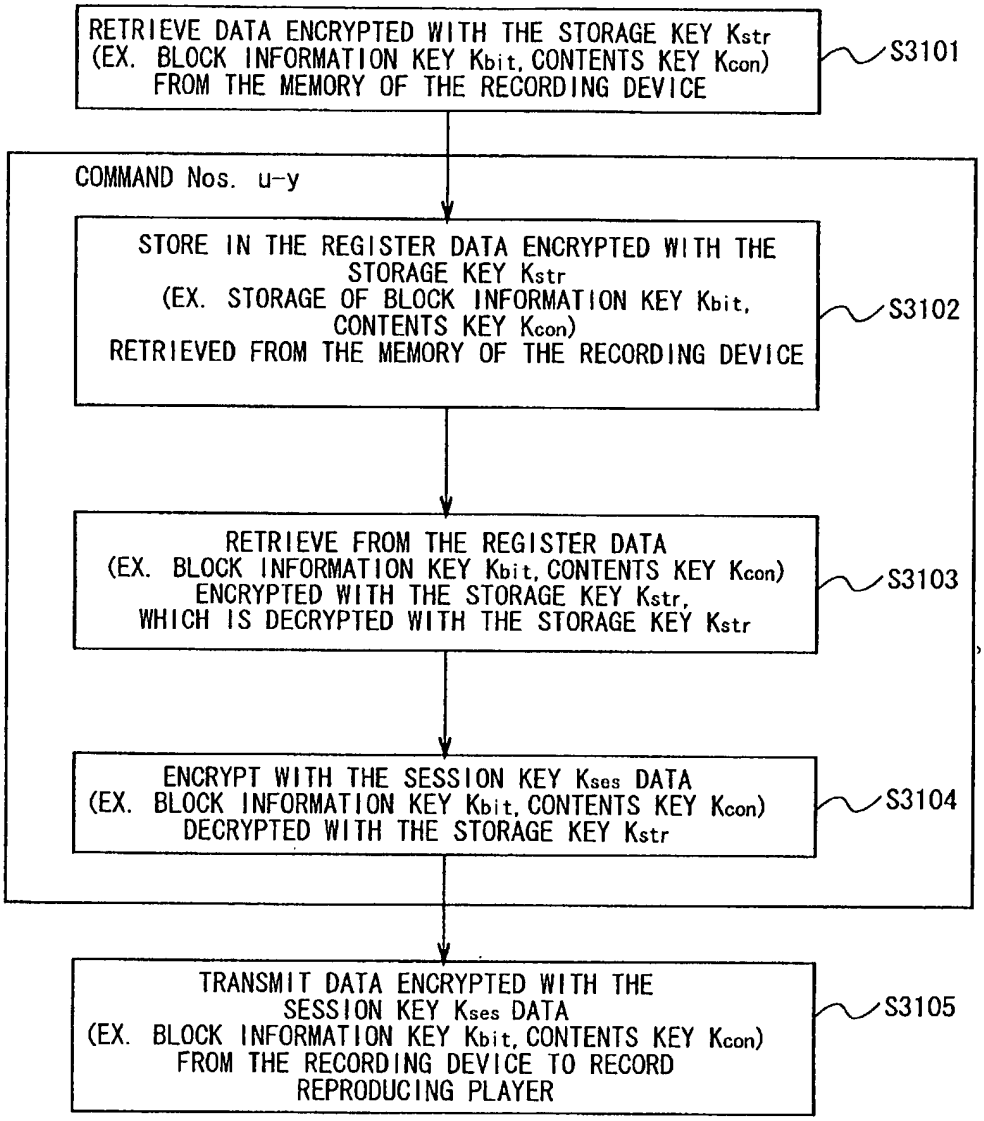

RETRIEVE DATA ENCRYPTED WITH THE STORAGE KEY Kstr (EX. BLOCK INFORMATION KEY Kbit, CONTENTS KEY Kcon) FROM THE MEMORY OF THE RECORDING DEVICE
S3101
COMMAND Nos. u-y
STORE IN THE REGISTER DATA ENCRYPTED WITH THE STORAGE KEY Kstr (EX. STORAGE OF BLOCK INFORMATION KEY Kbit, CONTENTS KEY Kcon) RETRIEVED FROM THE MEMORY OF THE RECORDING DEVICE
S3102
RETRIEVE FROM THE REGISTER DATA (EX. BLOCK INFORMATION KEY Kbit, CONTENTS KEY Kcon) ENCRYPTED WITH THE STORAGE KEY Kstr, WHICH IS DECRYPTED WITH THE STORAGE KEY Kstr
S3103
ENCRYPT WITH THE SESSION KEY Kses DATA (EX. BLOCK INFORMATION KEY Kbit, CONTENTS KEY Kcon) DECRYPTED WITH THE STORAGE KEY Kstr
S3104
TRANSMIT DATA ENCRYPTED WITH THE SESSION KEY Kses DATA (EX. BLOCK INFORMATION KEY Kbit, CONTENTS KEY Kcon) FROM THE RECORDING DEVICE TO RECORD REPRODUCING PLAYER
S3105

FIG. 31

FORMAT TYPE 0

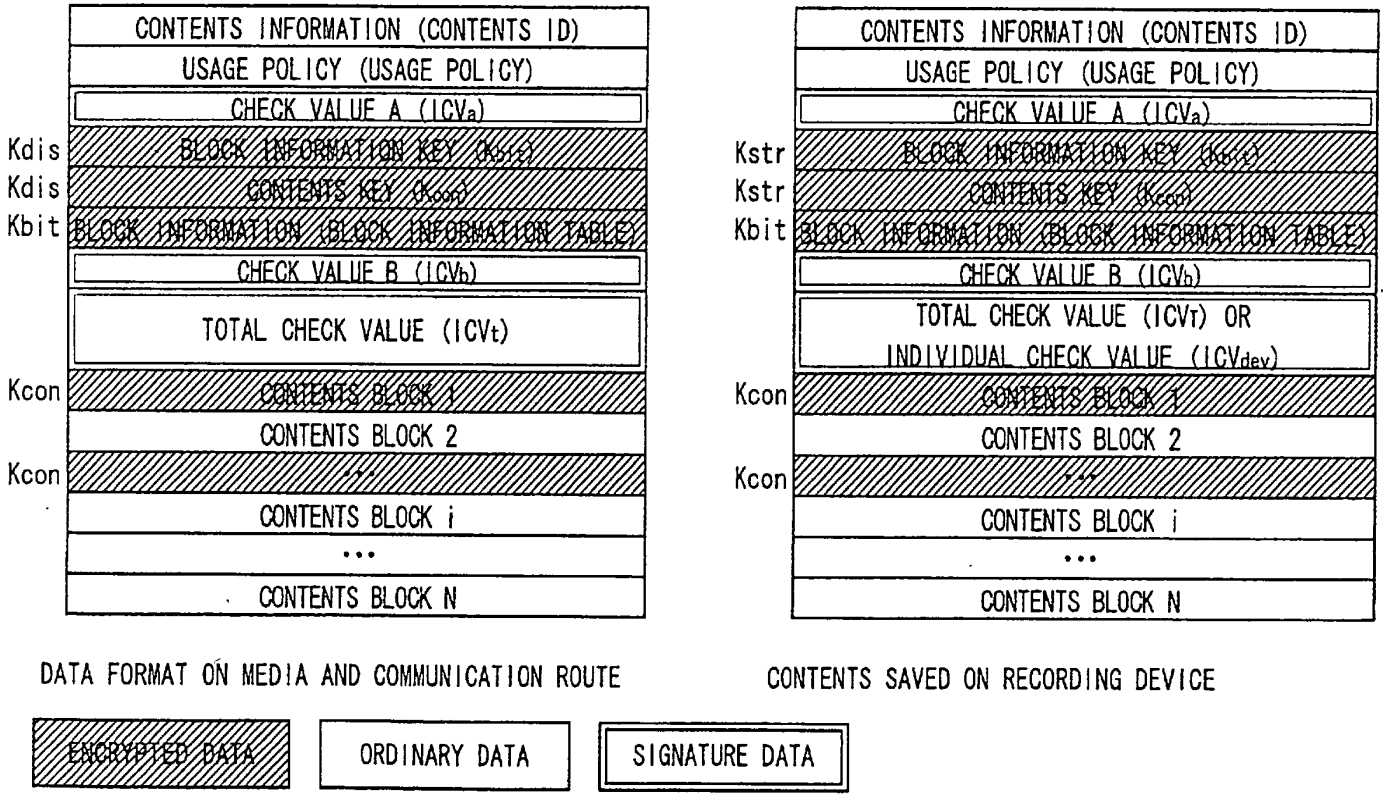


FIG. 32

FORMAT TYPE 1

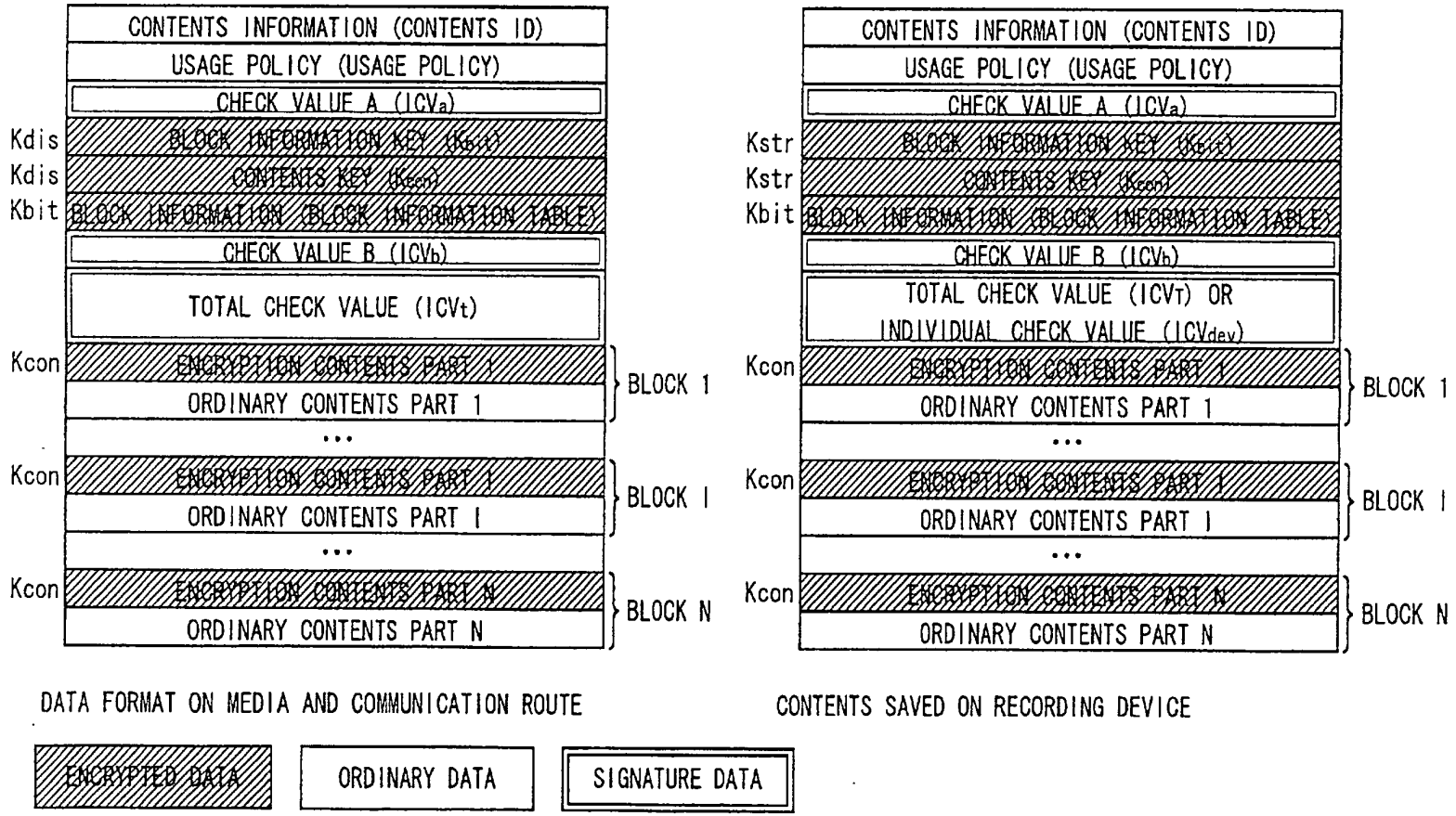


FIG. 33

FORMAT TYPE 2

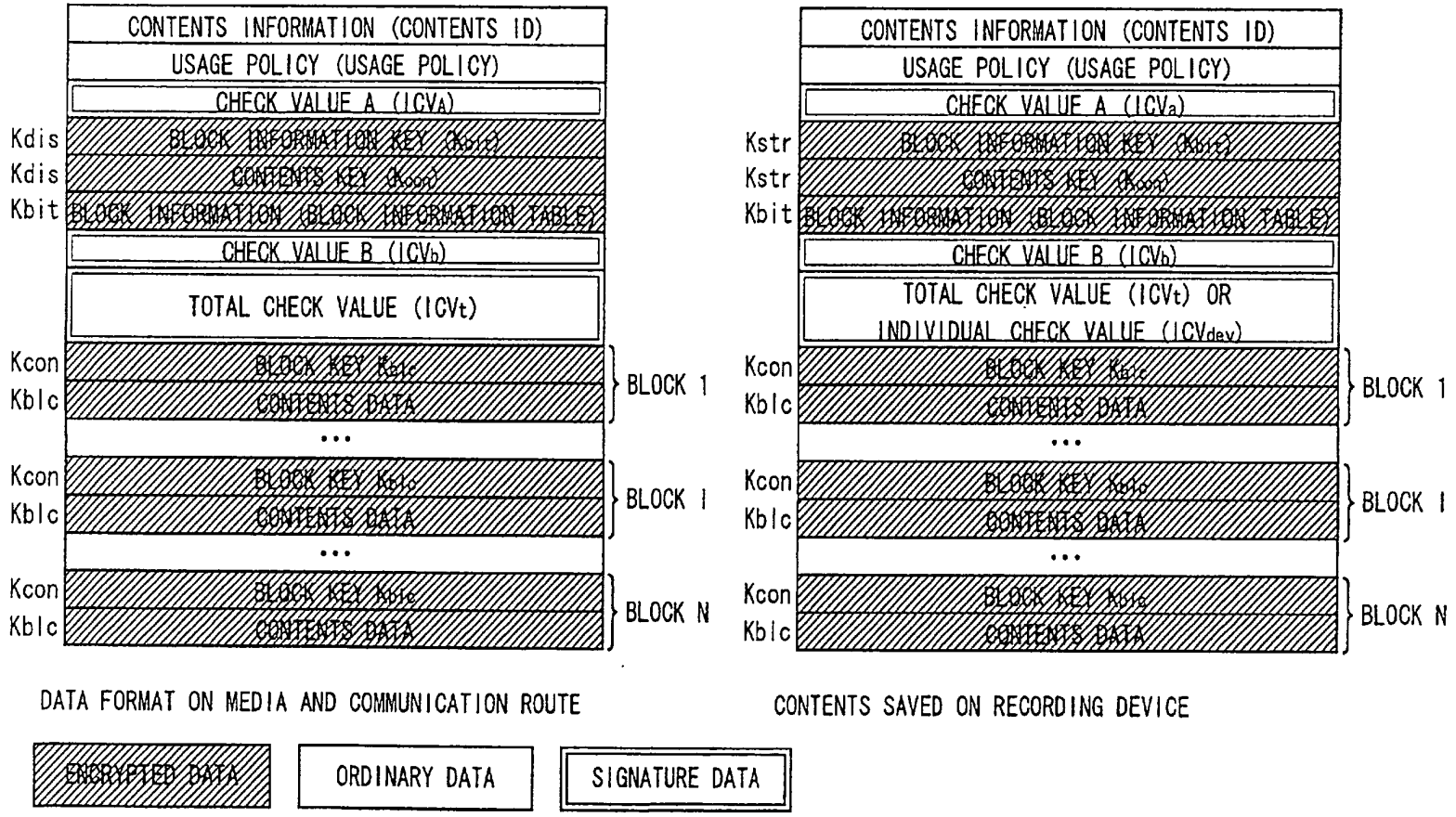


FIG. 34

FORMAT TYPE 3

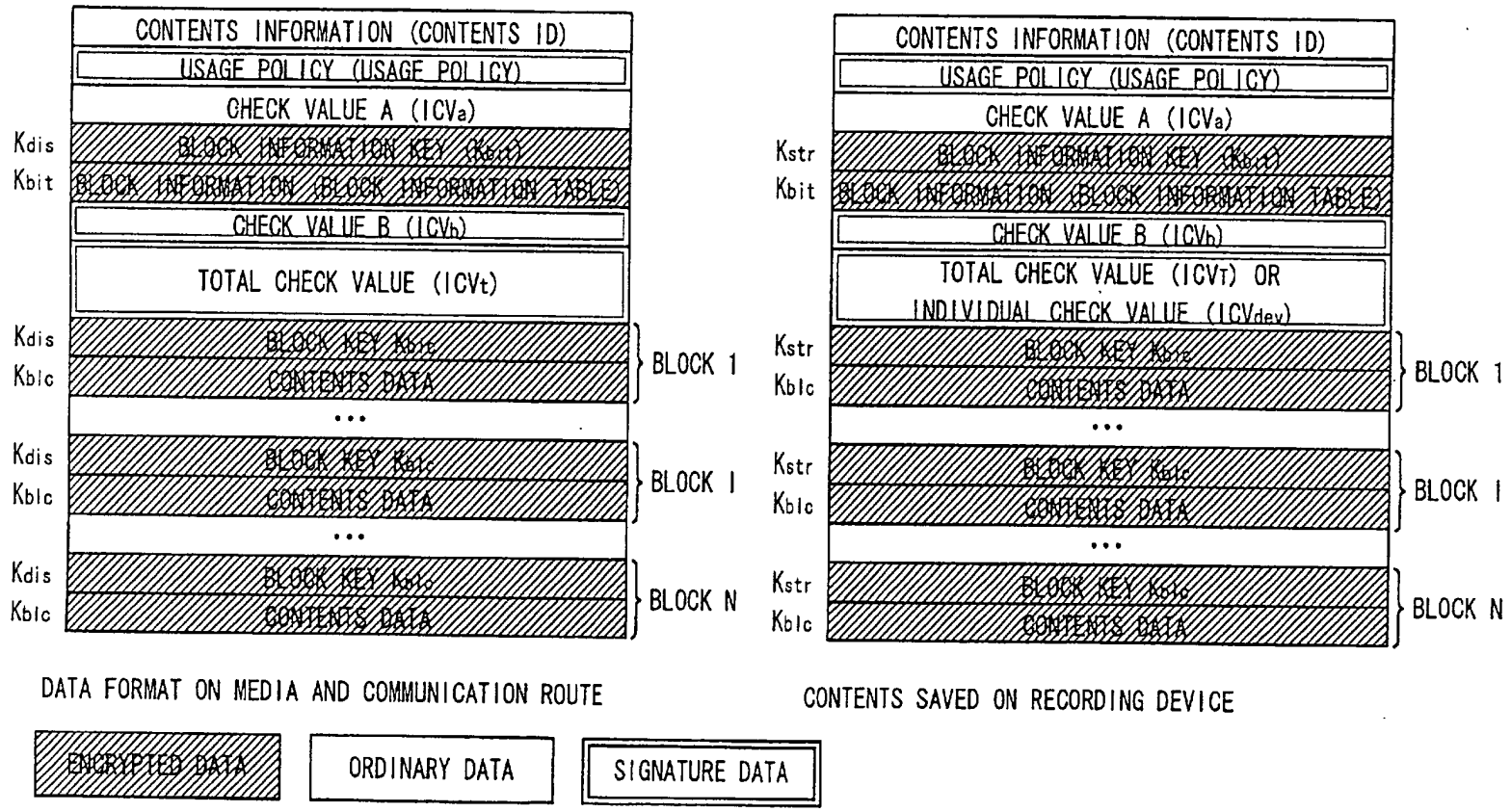
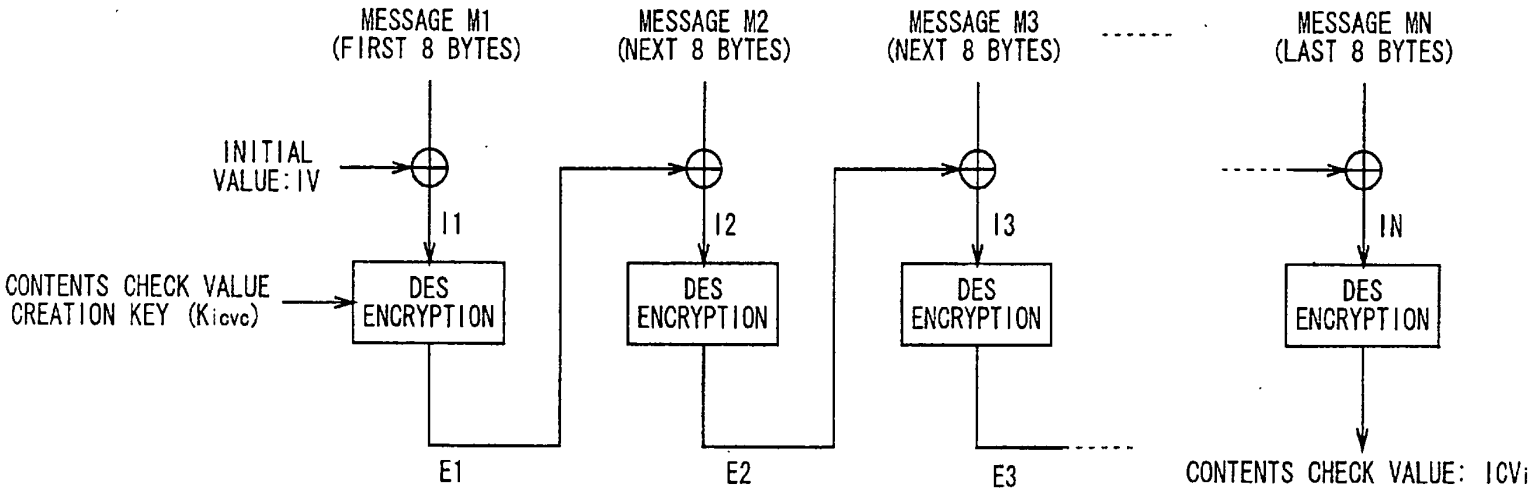


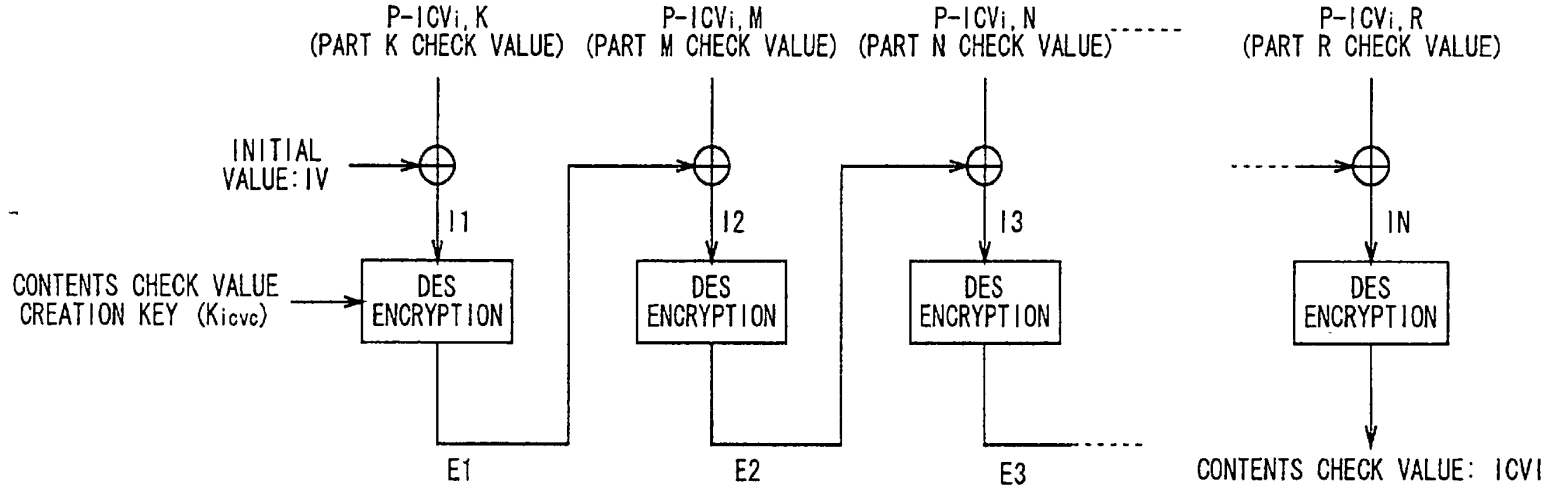
FIG. 35



MESSAGE M1 - MN: CONTENTS DATE OF CONTENTS I

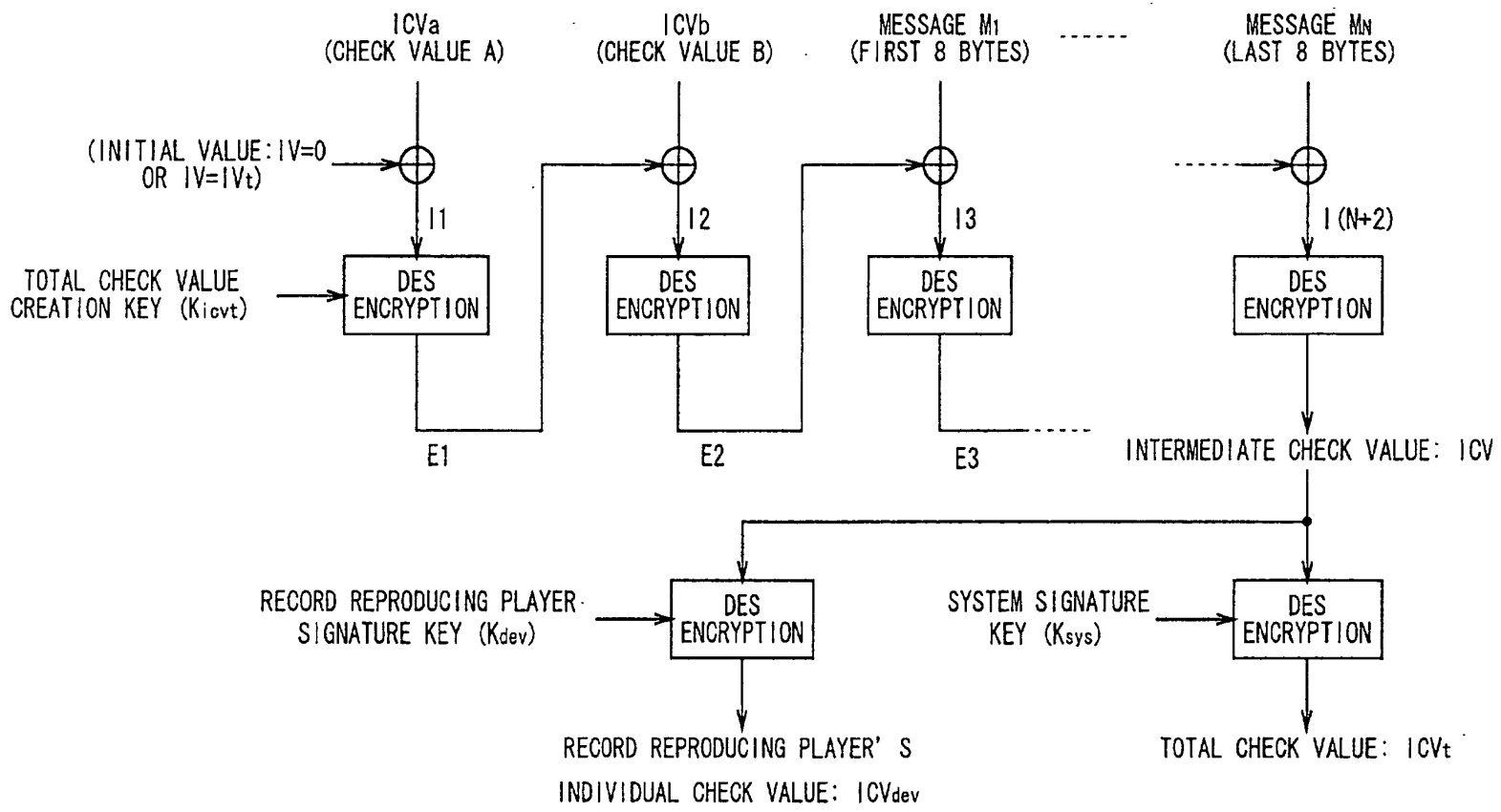
⊕:EXCLUSIVE OR (XOR) PROCESS (8-BYTE UNIT)

FIG. 36



⊕:EXCLUSIVE OR (XOR) PROCESS (8-BYTE UNIT)

FIG. 37



MESSAGE M1 - MN: DATA OF CONTENTS BLOCK 1 ~ N

⊕:EXCLUSIVE OR (XOR) PROCESS (8-BYTE UNIT)

FIG. 38

FORMAT TYPE 0, 1 DOWNLOADING PROCESS

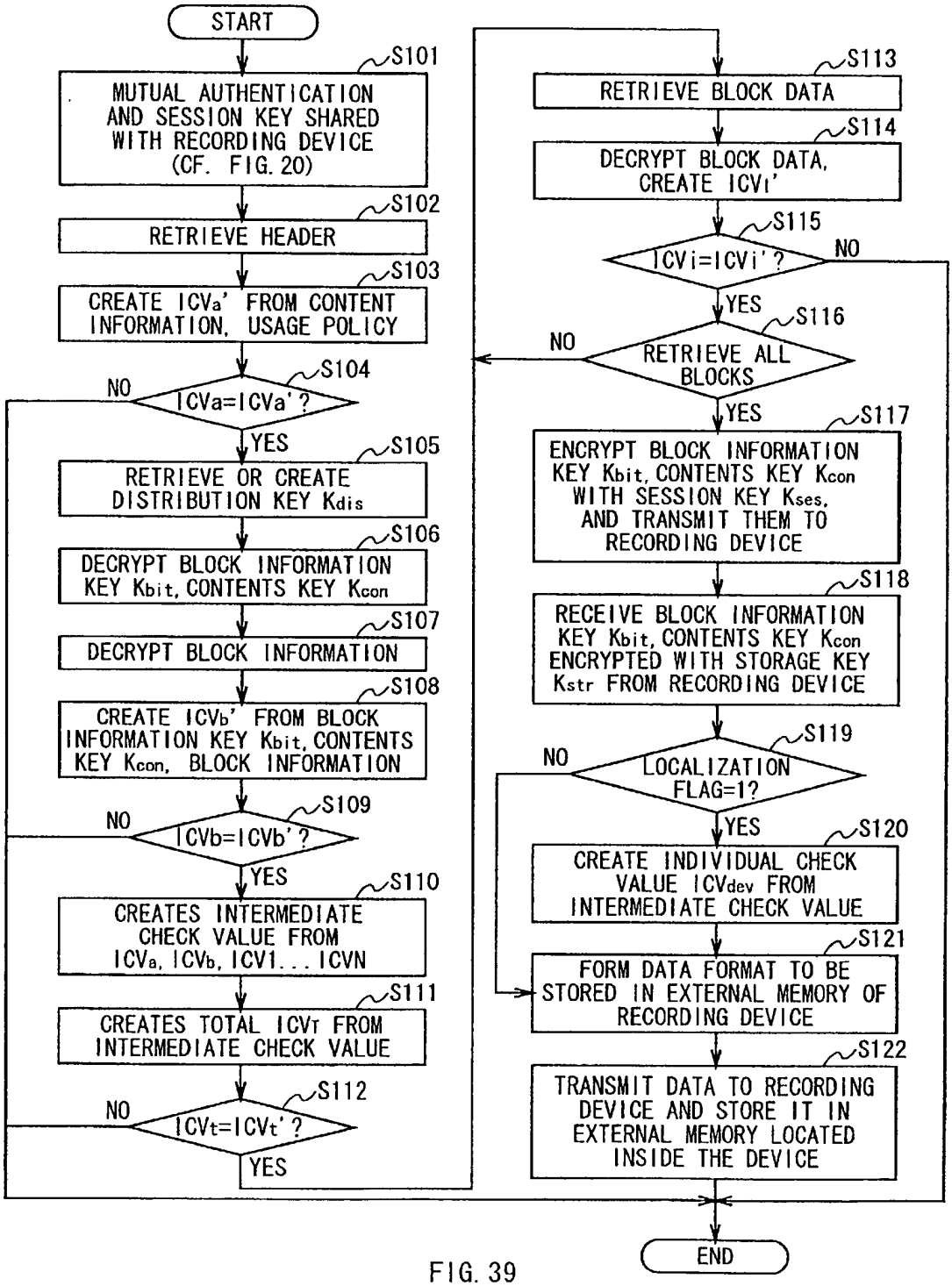


FIG. 39

FORMAT TYPE 2 DOWNLOADING PROCESS

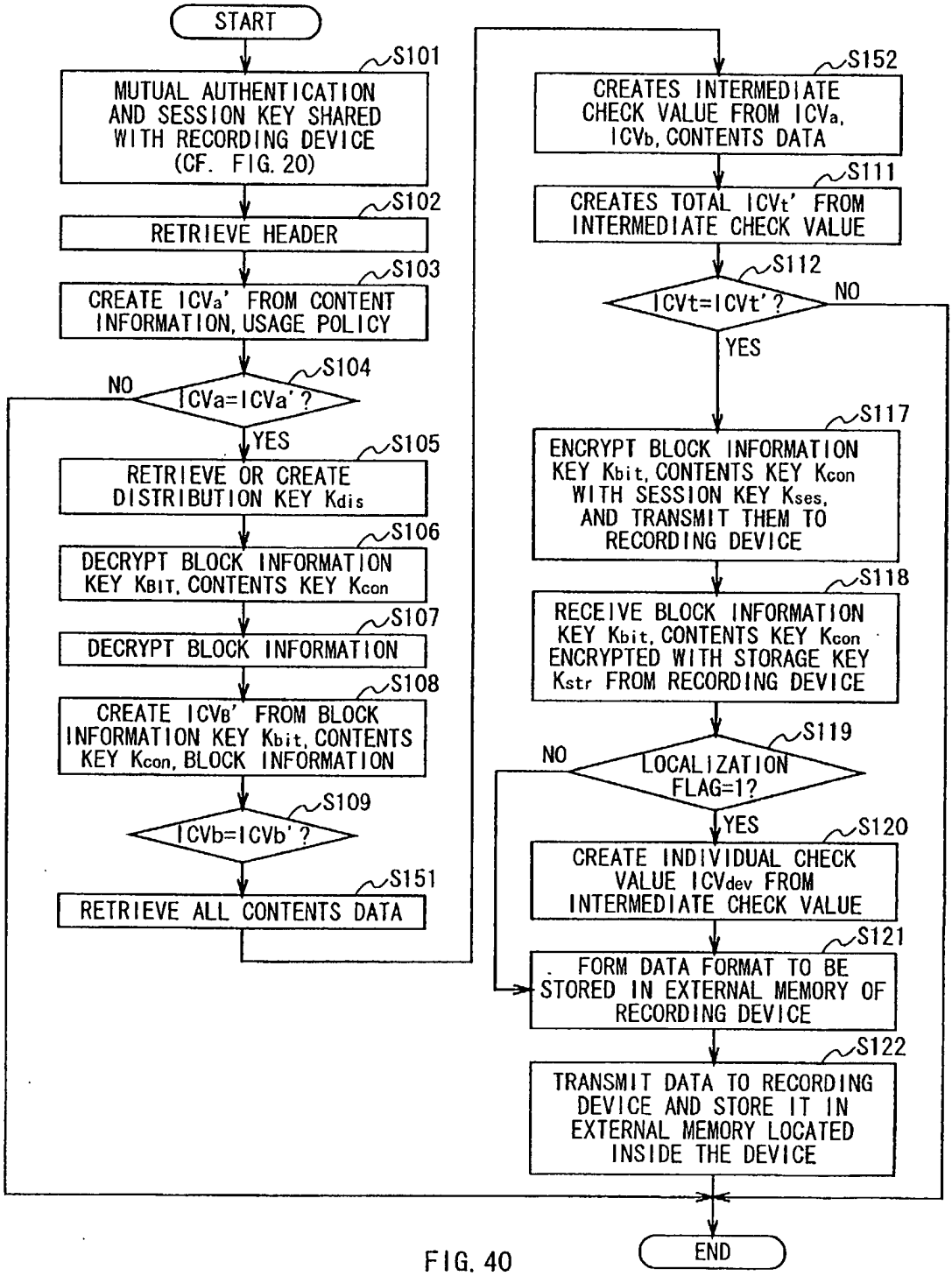


FIG. 40

FORMAT TYPE 3 DOWNLOADING PROCESS

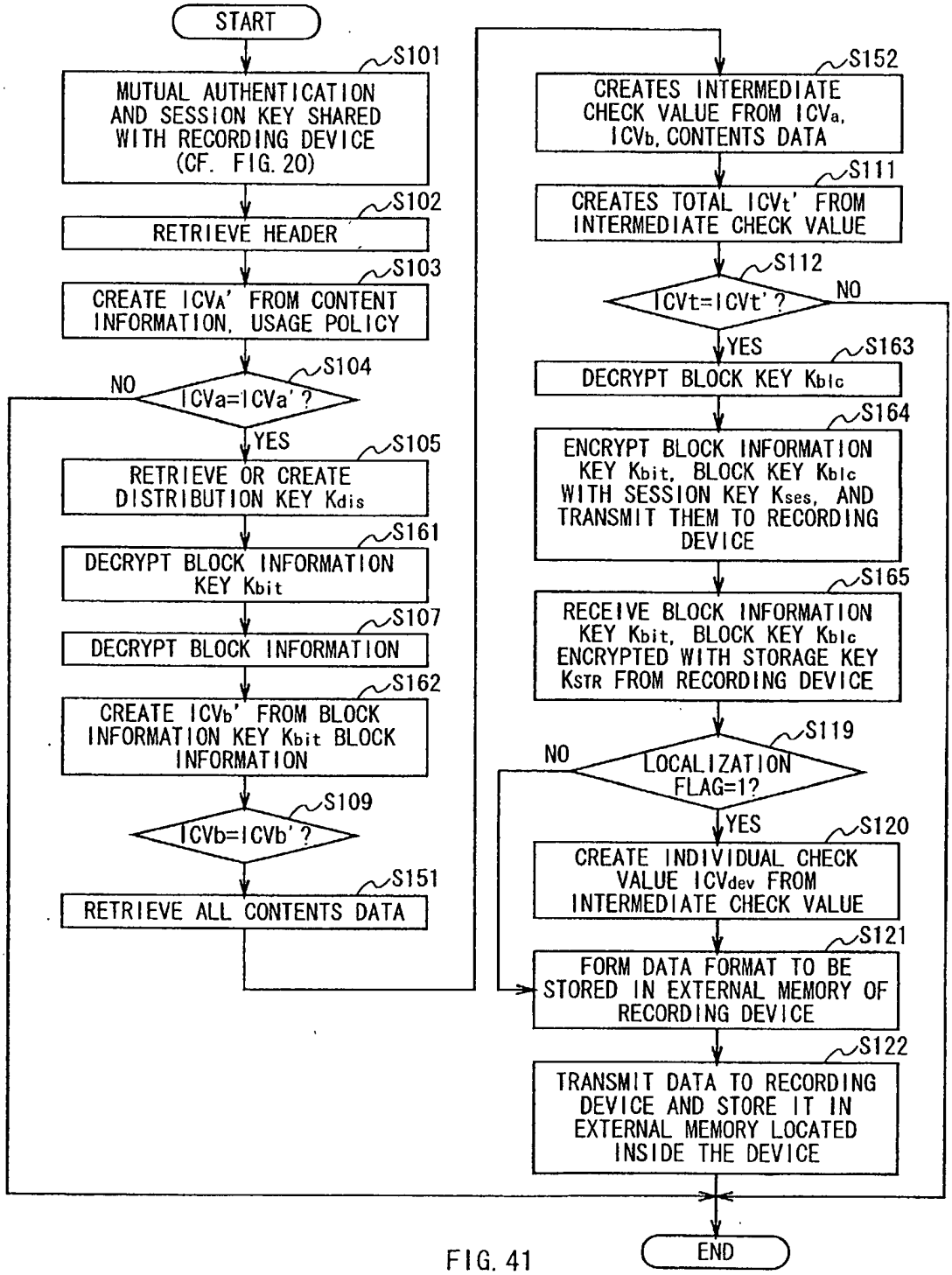


FIG. 41

FORMAT TYPE 4 DOWNLOADING PROCESS

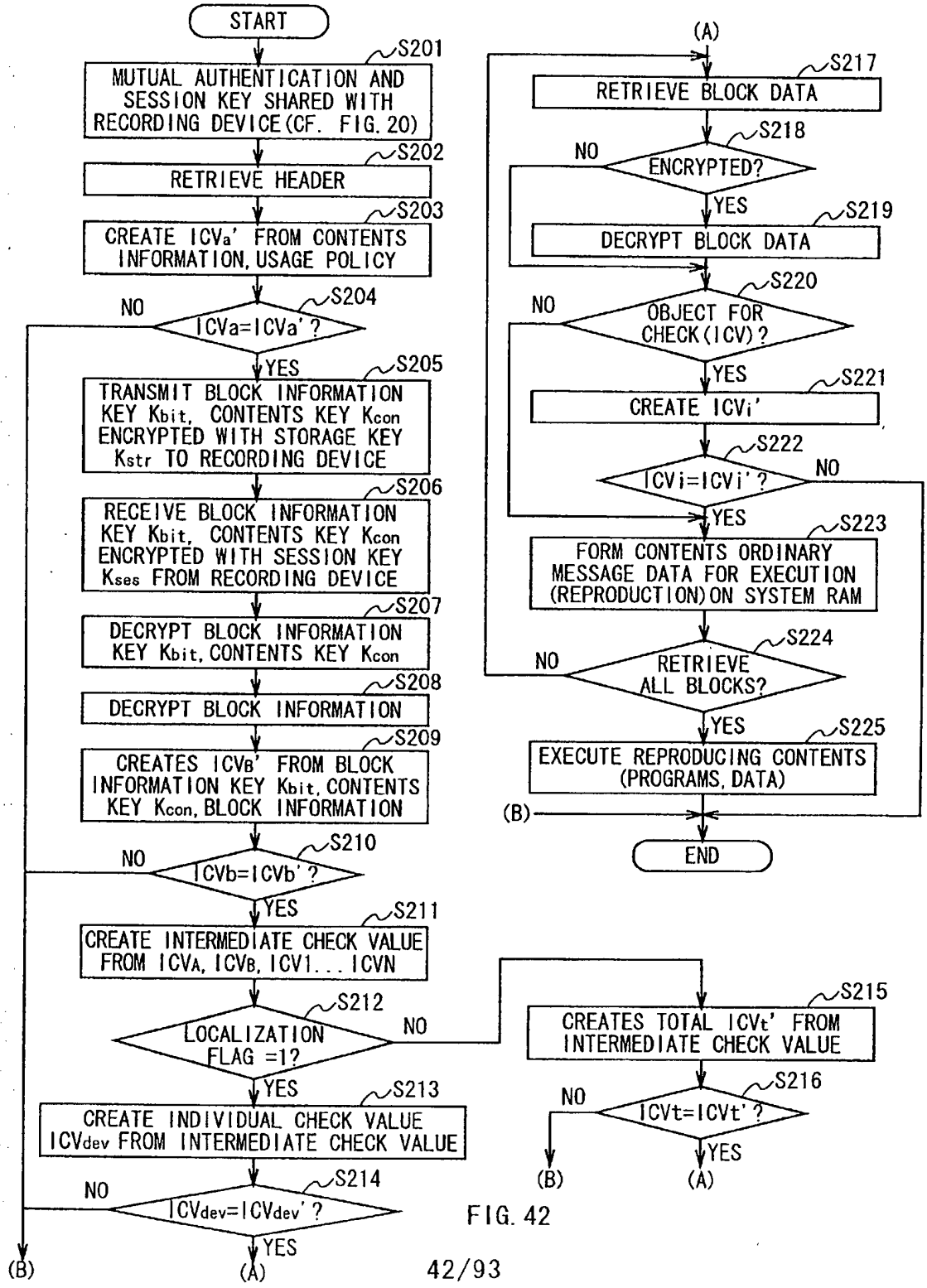


FIG. 42

FORMAT TYPE 1 REPRODUCTION PROCESS

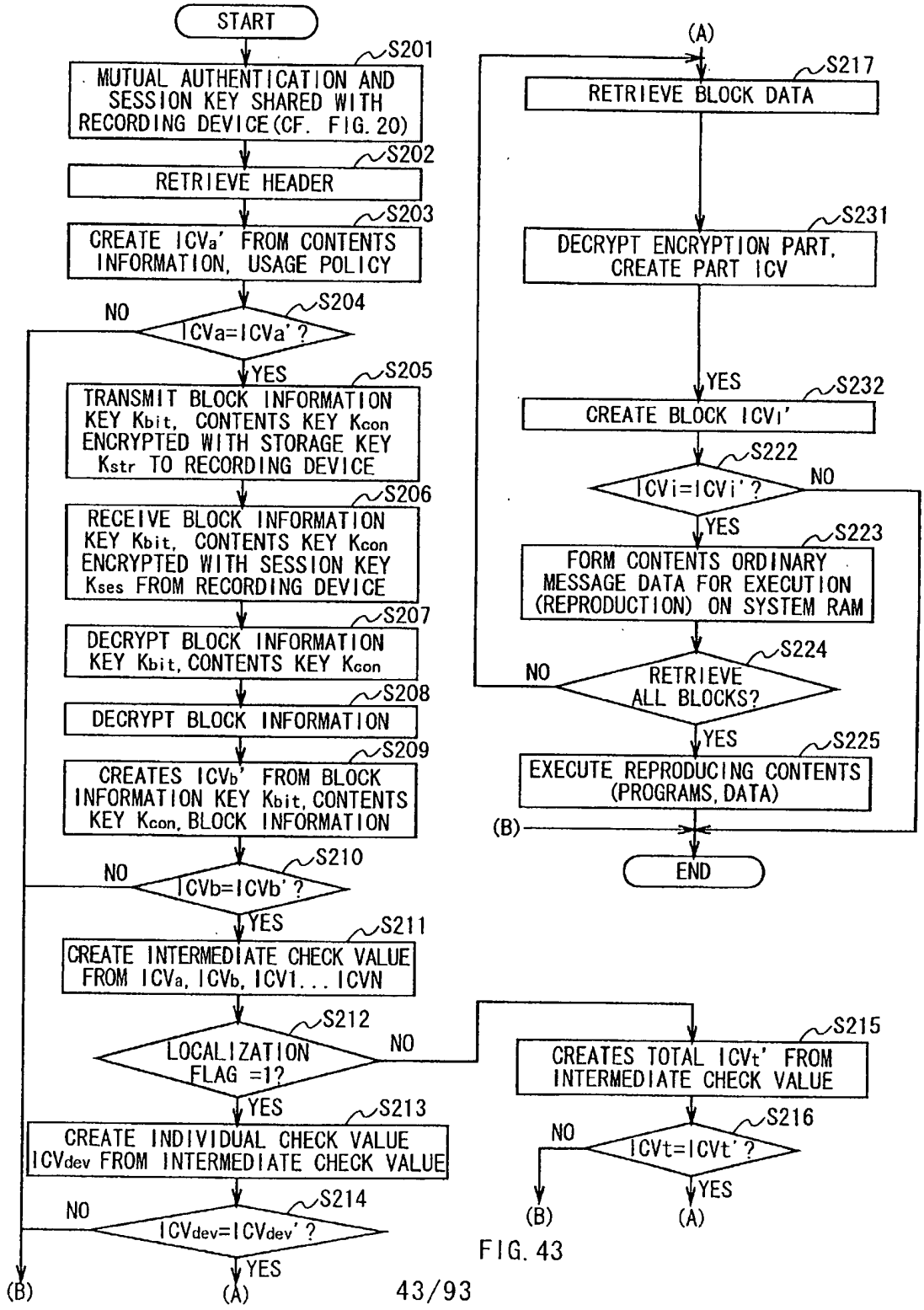


FIG. 43

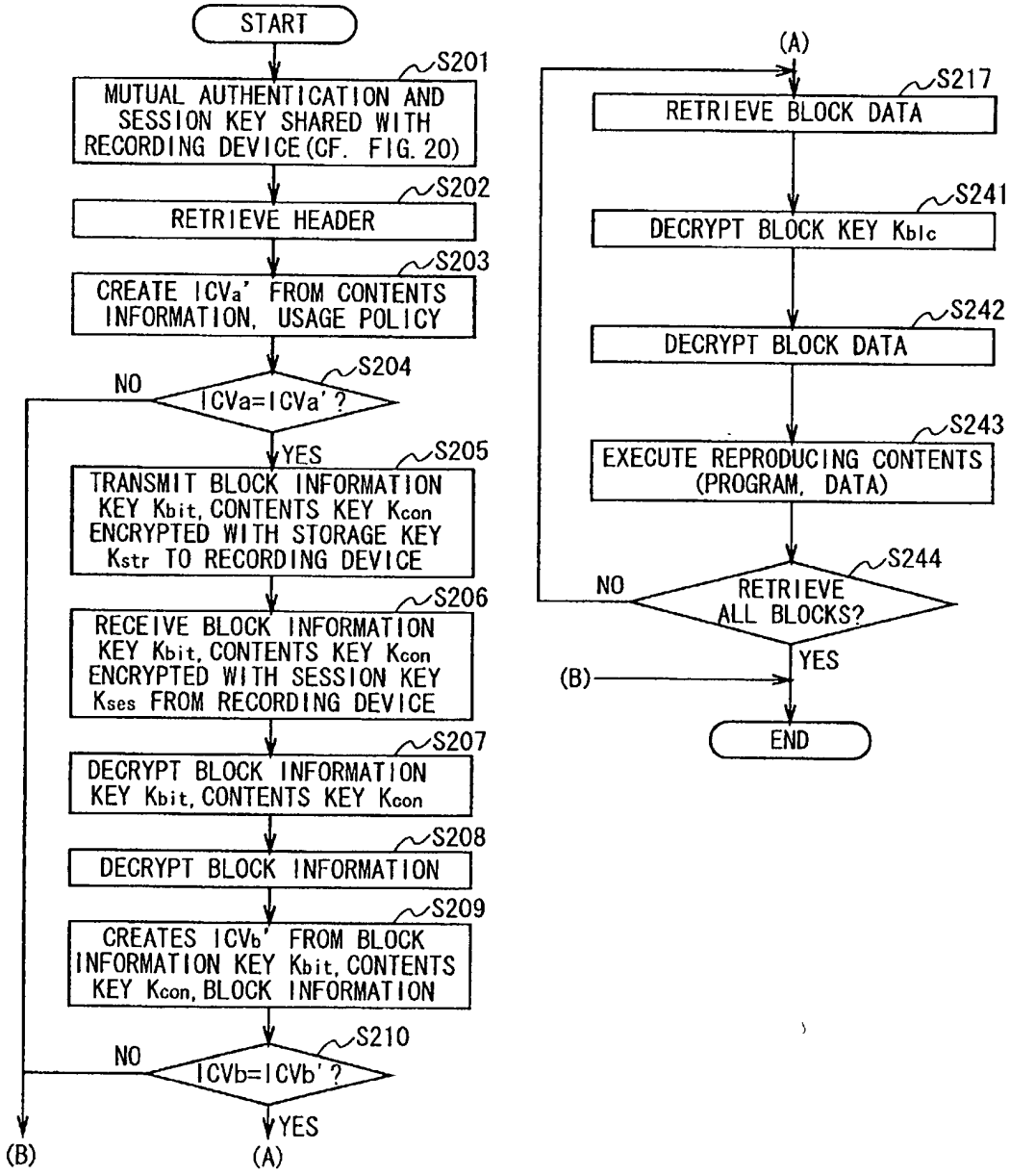

START
S201
MUTUAL AUTHENTICATION AND SESSION KEY SHARED WITH RECORDING DEVICE (CF. FIG. 20)
S202
RETRIEVE HEADER
S203
CREATE ICVa' FROM CONTENTS INFORMATION, USAGE POLICY
S204
NO
ICVa=ICVa'?
YES
S205
TRANSMIT BLOCK INFORMATION KEY Kbit, CONTENTS KEY Kcon ENCRYPTED WITH STORAGE KEY Kstr TO RECORDING DEVICE
S206
RECEIVE BLOCK INFORMATION KEY Kbit, CONTENTS KEY Kcon ENCRYPTED WITH SESSION KEY Kses FROM RECORDING DEVICE
S207
DECRYPT BLOCK INFORMATION KEY Kbit, CONTENTS KEY Kcon
S208
DECRYPT BLOCK INFORMATION
S209
CREATES ICVb' FROM BLOCK INFORMATION KEY Kbit, CONTENTS KEY Kcon, BLOCK INFORMATION
S210
NO
ICVb=ICVb'?
YES
(B)
(A)
(A)
S217
RETRIEVE BLOCK DATA
S241
DECRYPT BLOCK KEY Kblc
S242
DECRYPT BLOCK DATA
S243
EXECUTE REPRODUCING CONTENTS (PROGRAM, DATA)
S244
NO
RETRIEVE ALL BLOCKS?
YES
(B)
END

FIG. 44

FORMAT TYPE 3 REPRODUCTION PROCESS

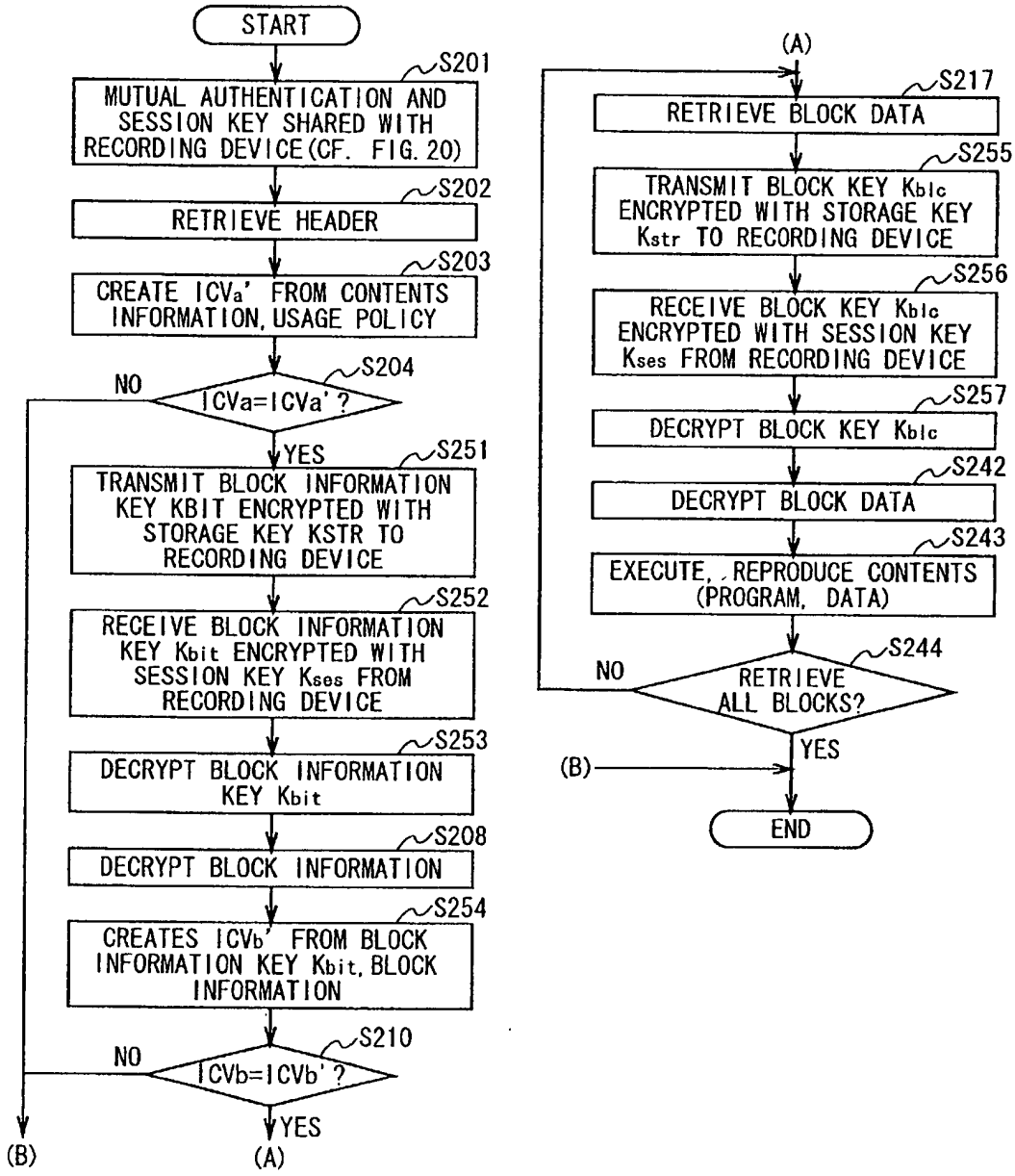


FIG. 45

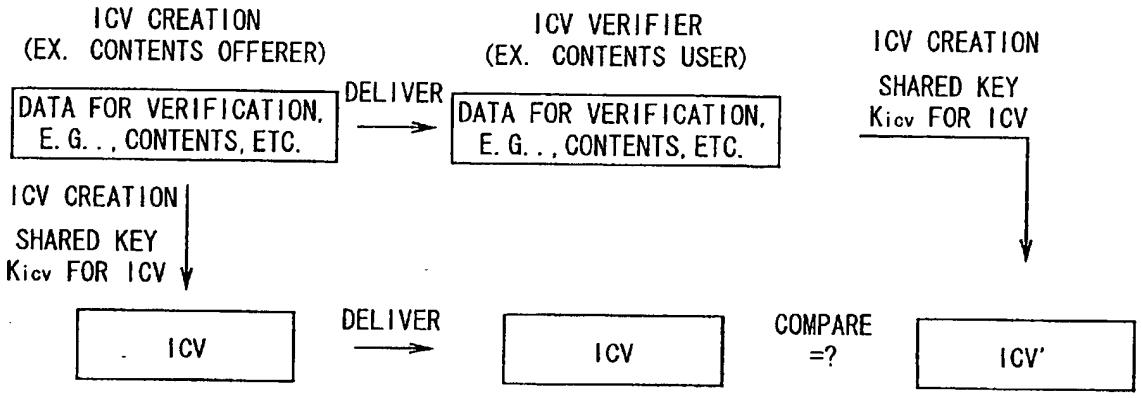

ICV CREATION
(EX. CONTENTS OFFERER)
ICV VERIFIER
(EX. CONTENTS USER)
ICV CREATION
SHARED KEY
Kicv FOR ICV
DATA FOR VERIFICATION, E.G., CONTENTS, ETC.
DELIVER
DATA FOR VERIFICATION, E.G., CONTENTS, ETC.
ICV CREATION
SHARED KEY
Kicv FOR ICV
ICV
DELIVER
ICV
COMPARE
=?
ICV'

FIG. 46

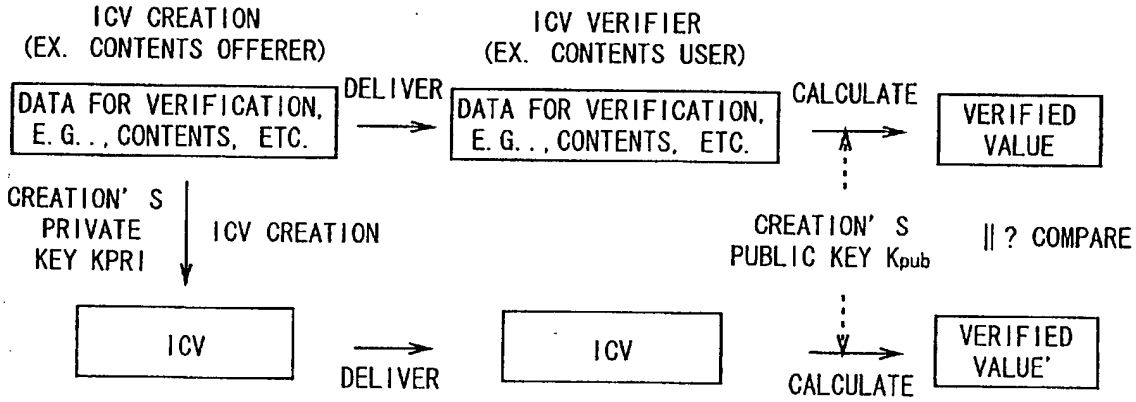
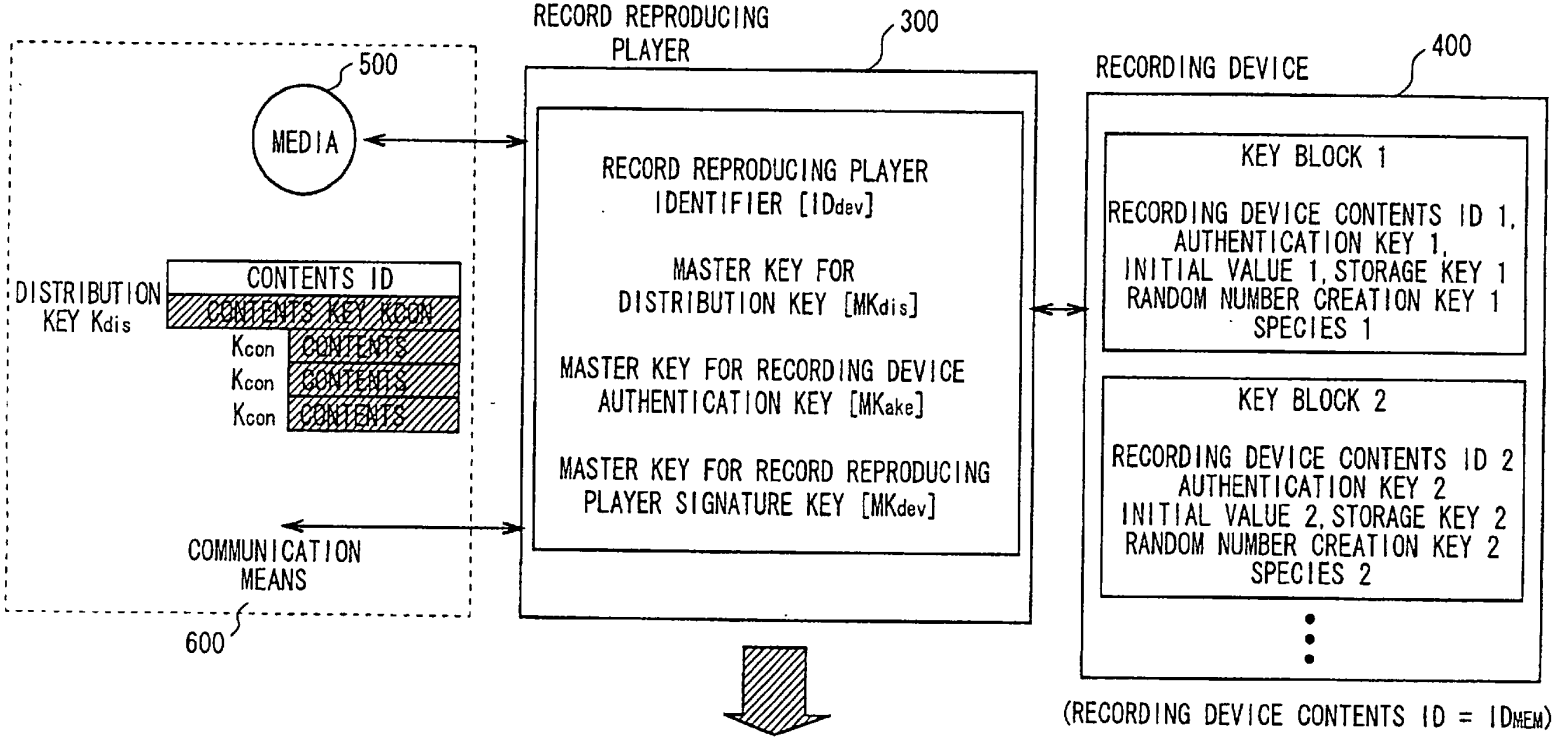

ICV CREATION
(EX. CONTENTS OFFERER)
ICV VERIFIER
(EX. CONTENTS USER)
DATA FOR VERIFICATION, E.G., CONTENTS, ETC.
DELIVER
DATA FOR VERIFICATION, E.G., CONTENTS, ETC.
CALCULATE
VERIFIED VALUE
CREATION' S PRIVATE KEY KPRI
ICV CREATION
CREATION' S PUBLIC KEY Kpub
|| ? COMPARE
ICV
DELIVER
ICV
CALCULATE
VERIFIED VALUE'

FIG. 47

CERTIFICATION CENTER
ICV
PUBLIC KEY (Kpub)
DELIVER
ICV VERIFIER
(EX. CONTENTS USER)
PUBLIC KEY (Kpub)
CALCULATE
VERIFIED VALUE 1
CENTER PRIVATE KEY FOR CREATION OF PUBLIC KEY CERTIFICATE SKpri
CERTIFICATE (= CENTER SIGNATURE)
DELIVER
CERTIFICATE (= CENTER SIGNATURE)
CENTER PUBLIC KEY SKpub
?
COMPARE
CALCULATE
VERIFIED VALUE 1'
ICV CREATION
(EX. CONTENTS OFFERER)
DATA FOR VERIFICATION, E.G.., CONTENTS, ETC.
DELIVER
DATA FOR VERIFICATION, E.G.., CONTENTS, ETC.
CALCULATE
VERIFIED VALUE 2
CREATION' S PRIVATE KEY Kpri
ICV CREATION
ICV
DELIVER
ICV
VERIFIED CREATION' S PUBLIC KEY Kpub
?
COMPARE
CALCULATE
VERIFIED VALUE 2'

FIG. 48



DISTRIBUTION KEY : $K_{DIS} = DES\ (MK_{dis},\ CONTENTS\ ID)$

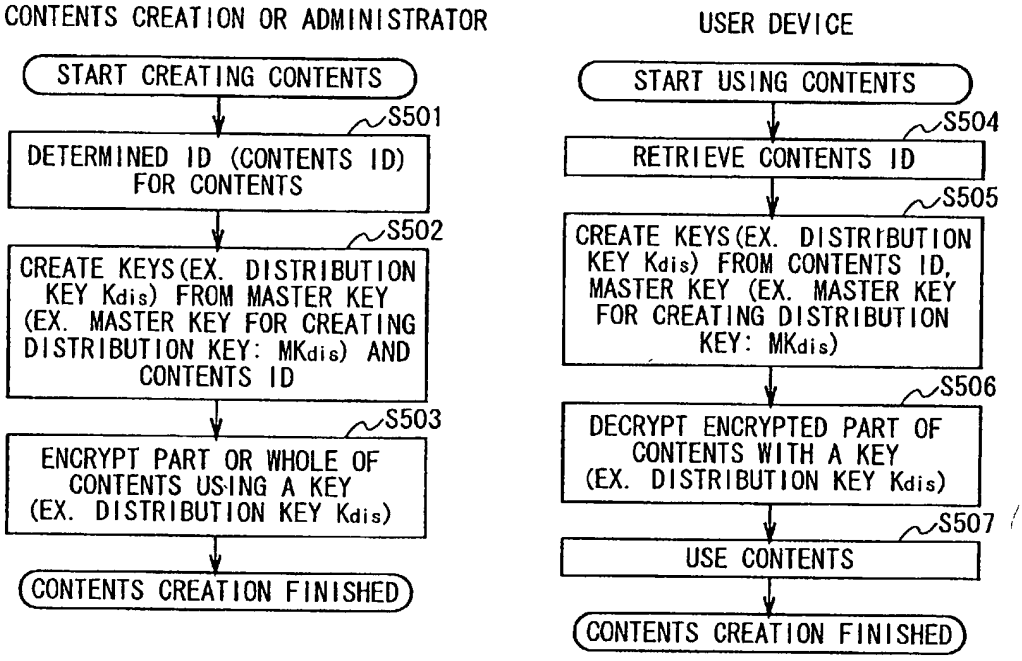
AUTHENTICATION KEY : $K_{ake} = DES\ (MK_{ake},\ ID_{mem})$

RECORD REPRIDUCING PLAYER SIGNATURE KEY : $K_{dev} = DES\ (MK_{dev},\ ID_{dev})$

FIG. 49

METHOD TO CREATE INDIVIDUAL KEYS FROM MASTER KEY-(1)

[BASIC FLOW]



[KEY POSSESSION COMPOSITION]

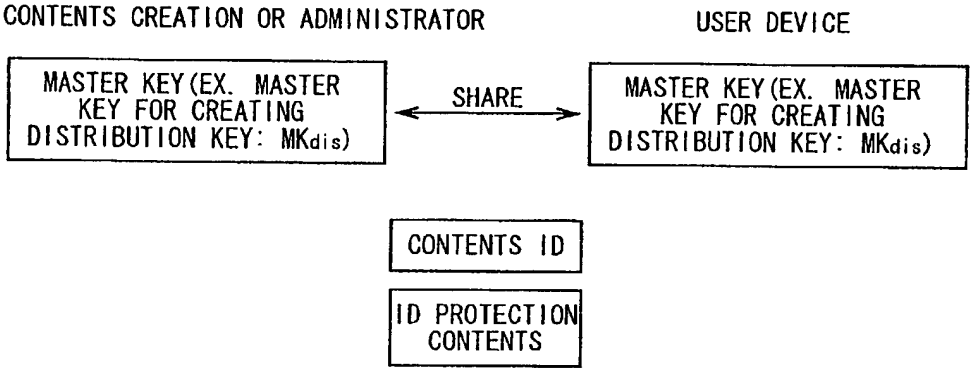
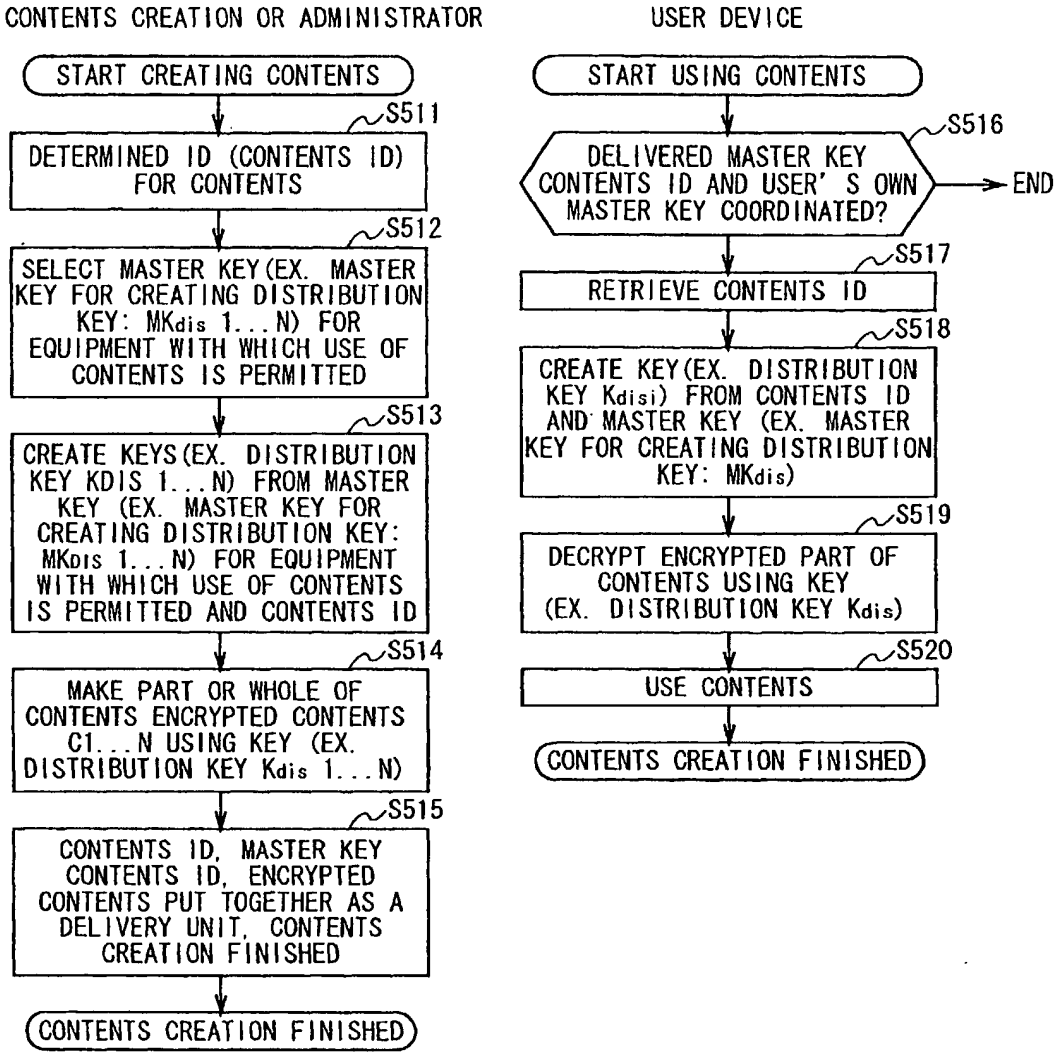


FIG. 50

METHOD TO CREATE INDIVIDUAL KEYS FROM MASTER KEY-(2)

[BASIC FLOW]



[KEY POSSESSION COMPOSITION]

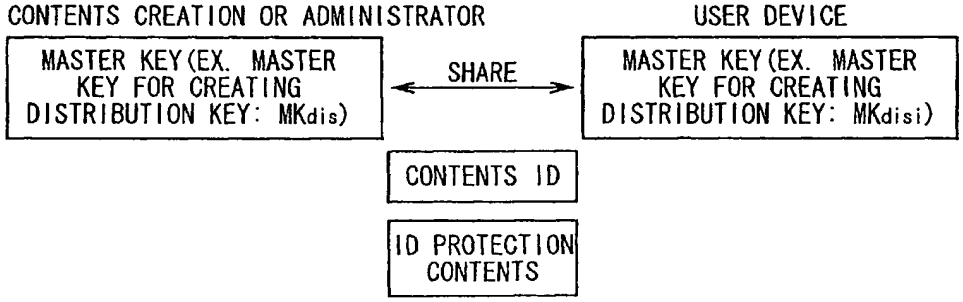


FIG. 51

CONTENTS PROVIDERS, ADMINISTRATORS

MASTER KEYS	ZONES	ENCRYPTED KEYS	ENCRYPTION (CONTENTS)
MK1	JAPAN	(MK1, CONTENTS ID)→K1	K1 (CONTENTS)
MK2	U. S.	(MK2, CONTENTS ID)→K2	K2 (CONTENTS)
MK3	EU	(MK3, CONTENTS ID)→K3	K3 (CONTENTS)
MK4	:	:	:
:	:	:	:

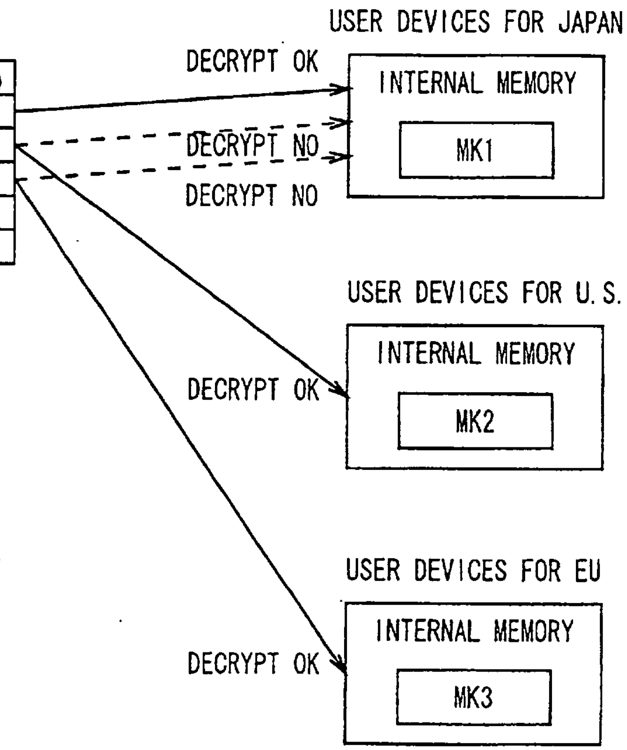


FIG. 52

METHOD TO CREATE INDIVIDUAL KEYS FROM MASTER KEY-(3)

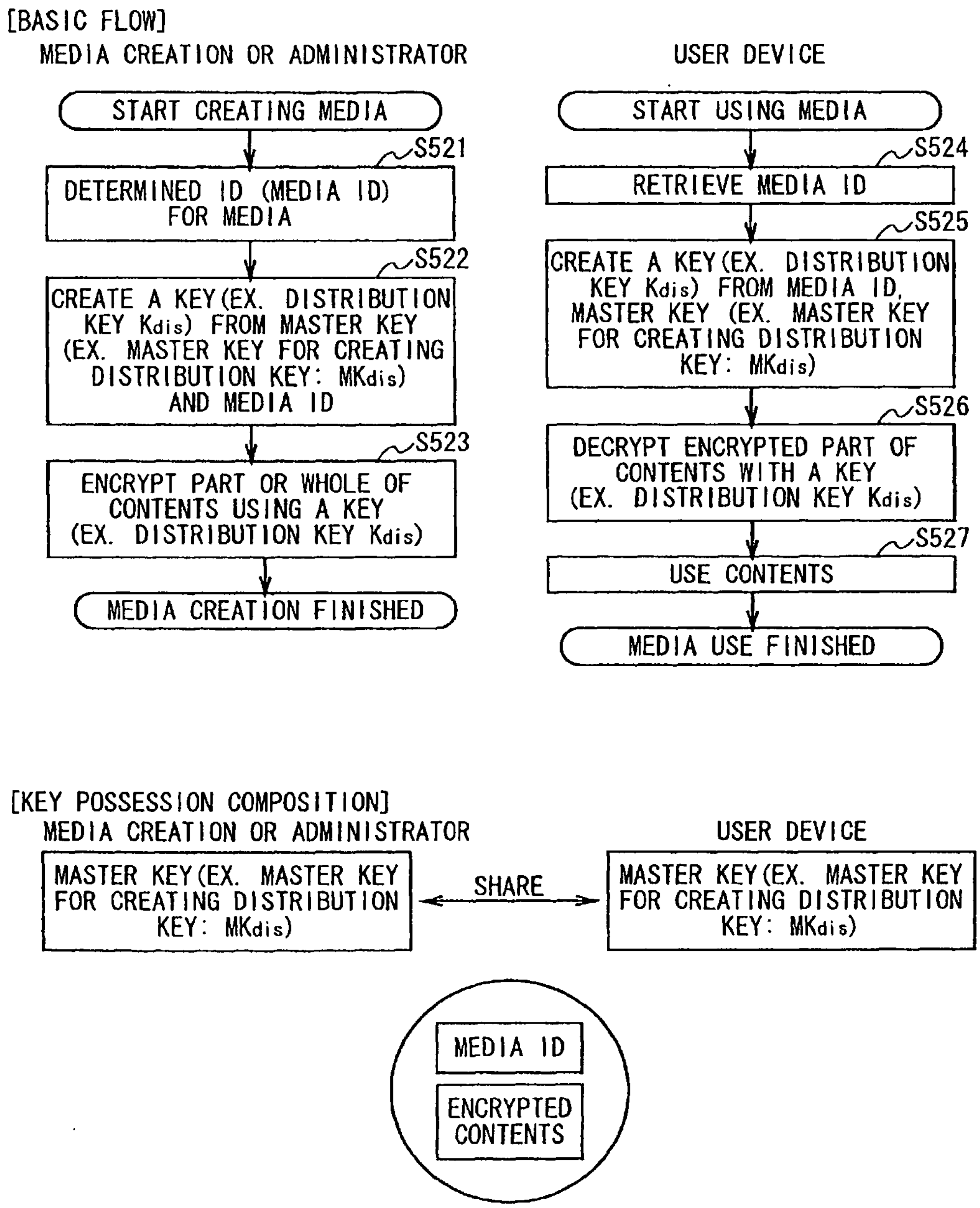
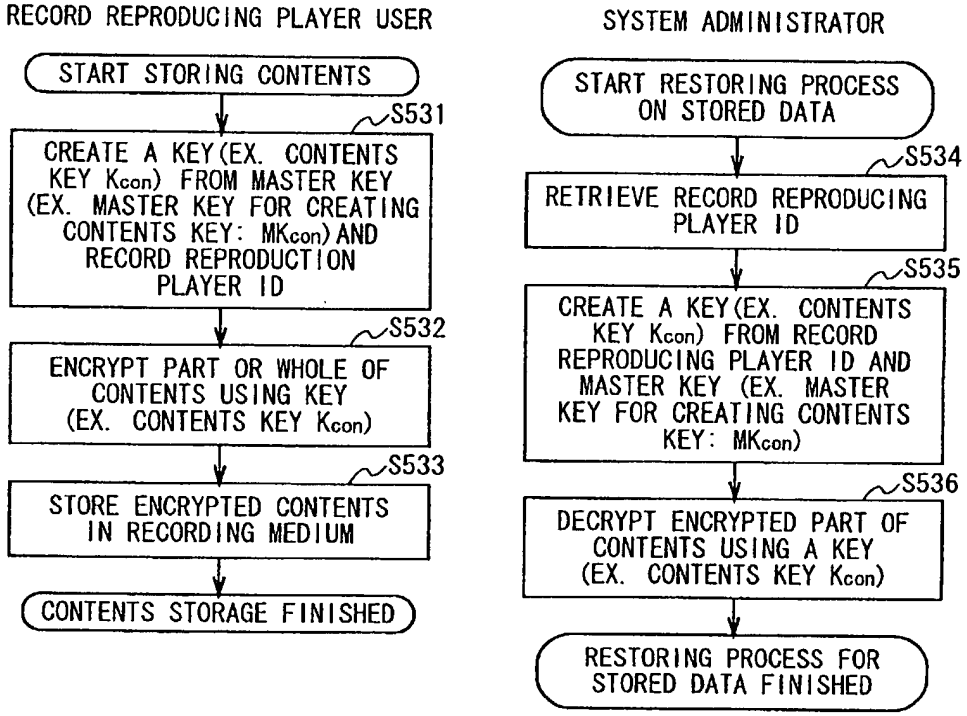


FIG. 53

METHOD TO CREATE INDIVIDUAL KEYS FROM MASTER KEY-(4)

[BASIC FLOW]



[KEY POSSESSION COMPOSITION]

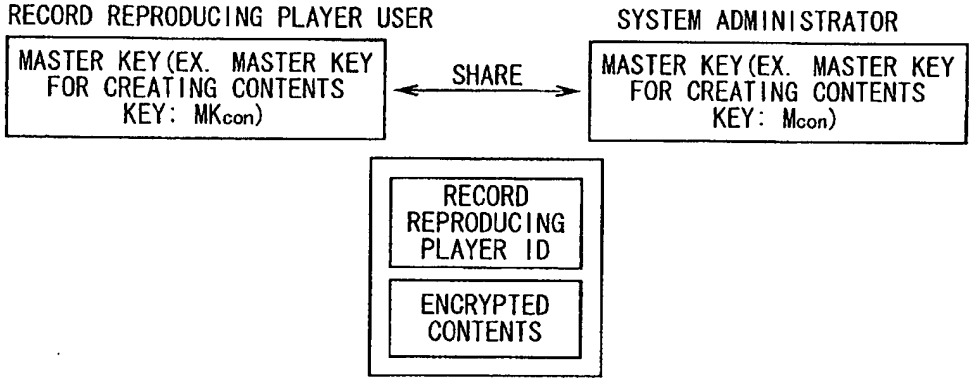
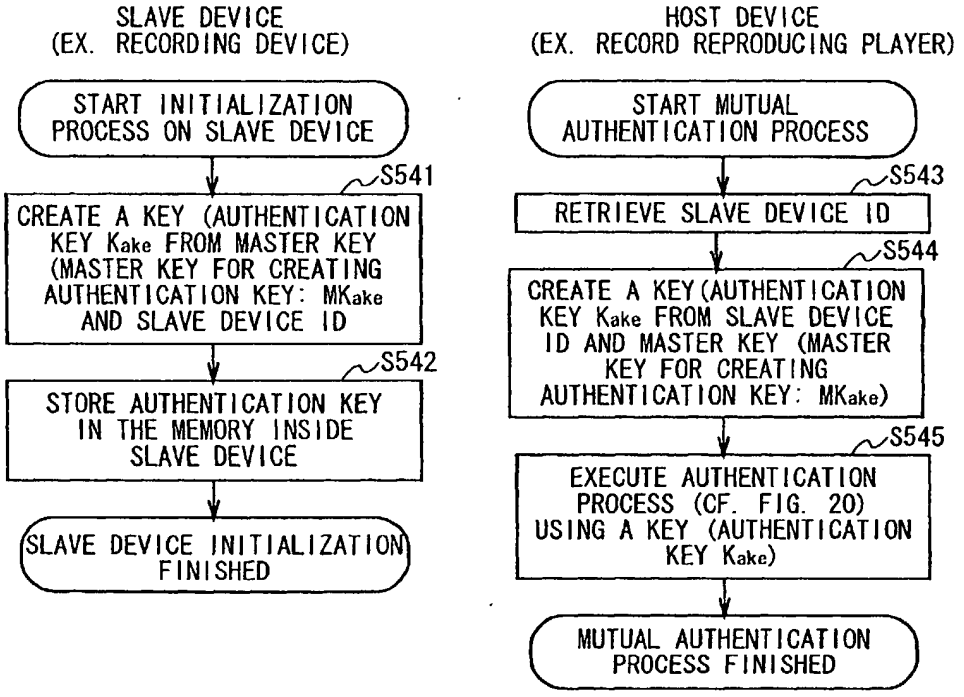


FIG. 54

METHOD TO CREATE INDIVIDUAL KEYS FROM MASTER KEY-(5)

[BASIC FLOW]



[KEY POSSESSION COMPOSITION]

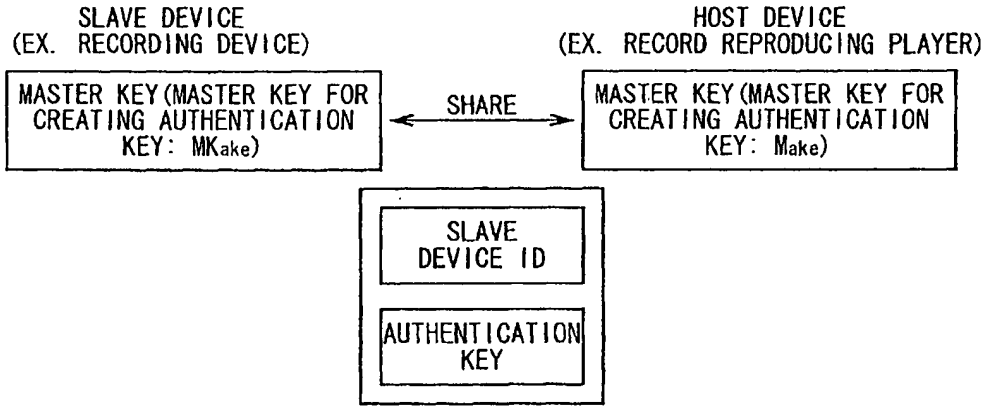


FIG. 55

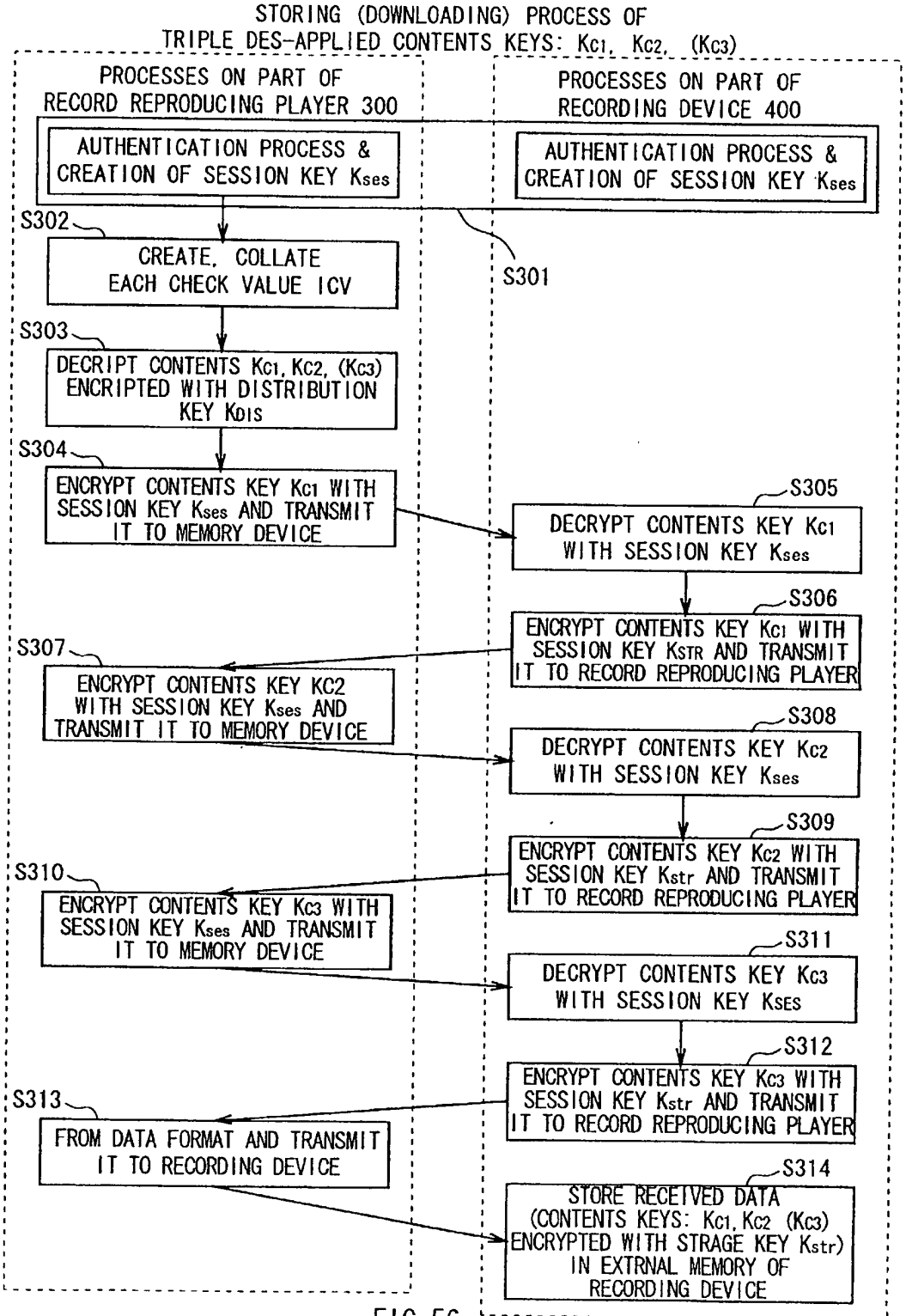

STORING (DOWNLOADING) PROCESS OF TRIPLE DES-APPLIED CONTENTS KEYS: Kc1, Kc2, (Kc3)
PROCESSES ON PART OF RECORD REPRODUCING PLAYER 300
PROCESSES ON PART OF RECORDING DEVICE 400
AUTHENTICATION PROCESS & CREATION OF SESSION KEY Kses
AUTHENTICATION PROCESS & CREATION OF SESSION KEY Kses
S301
S302
CREATE, COLLATE EACH CHECK VALUE ICV
S303
DECRIPT CONTENTS Kc1, Kc2, (Kc3) ENCRIPTED WITH DISTRIBUTION KEY KDIS
S304
ENCRYPT CONTENTS KEY Kc1 WITH SESSION KEY Kses AND TRANSMIT IT TO MEMORY DEVICE
S305
DECRYPT CONTENTS KEY Kc1 WITH SESSION KEY Kses
S306
ENCRYPT CONTENTS KEY Kc1 WITH SESSION KEY KSTR AND TRANSMIT IT TO RECORD REPRODUCING PLAYER
S307
ENCRYPT CONTENTS KEY KC2 WITH SESSION KEY Kses AND TRANSMIT IT TO MEMORY DEVICE
S308
DECRYPT CONTENTS KEY Kc2 WITH SESSION KEY Kses
S309
ENCRYPT CONTENTS KEY Kc2 WITH SESSION KEY Kstr AND TRANSMIT IT TO RECORD REPRODUCING PLAYER
S310
ENCRYPT CONTENTS KEY Kc3 WITH SESSION KEY Kses AND TRANSMIT IT TO MEMORY DEVICE
S311
DECRYPT CONTENTS KEY Kc3 WITH SESSION KEY KSES
S312
ENCRYPT CONTENTS KEY Kc3 WITH SESSION KEY Kstr AND TRANSMIT IT TO RECORD REPRODUCING PLAYER
S313
FROM DATA FORMAT AND TRANSMIT IT TO RECORDING DEVICE
S314
STORE RECEIVED DATA (CONTENTS KEYS: Kc1, Kc2 (Kc3) ENCRYPTED WITH STRAGE KEY Kstr) IN EXTRNAL MEMORY OF RECORDING DEVICE

FIG. 56

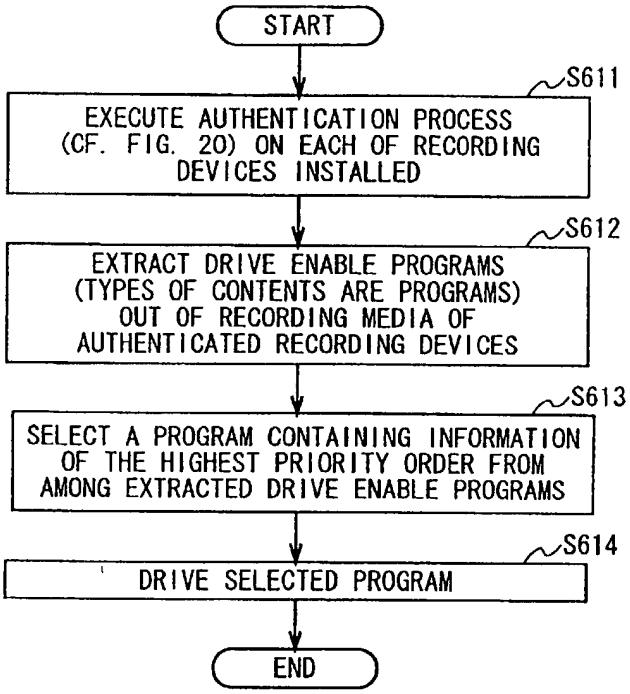

START
S611
EXECUTE AUTHENTICATION PROCESS (CF. FIG. 20) ON EACH OF RECORDING DEVICES INSTALLED
S612
EXTRACT DRIVE ENABLE PROGRAMS (TYPES OF CONTENTS ARE PROGRAMS) OUT OF RECORDING MEDIA OF AUTHENTICATED RECORDING DEVICES
S613
SELECT A PROGRAM CONTAINING INFORMATION OF THE HIGHEST PRIORITY ORDER FROM AMONG EXTRACTED DRIVE ENABLE PROGRAMS
S614
DRIVE SELECTED PROGRAM
END

FIG. 57

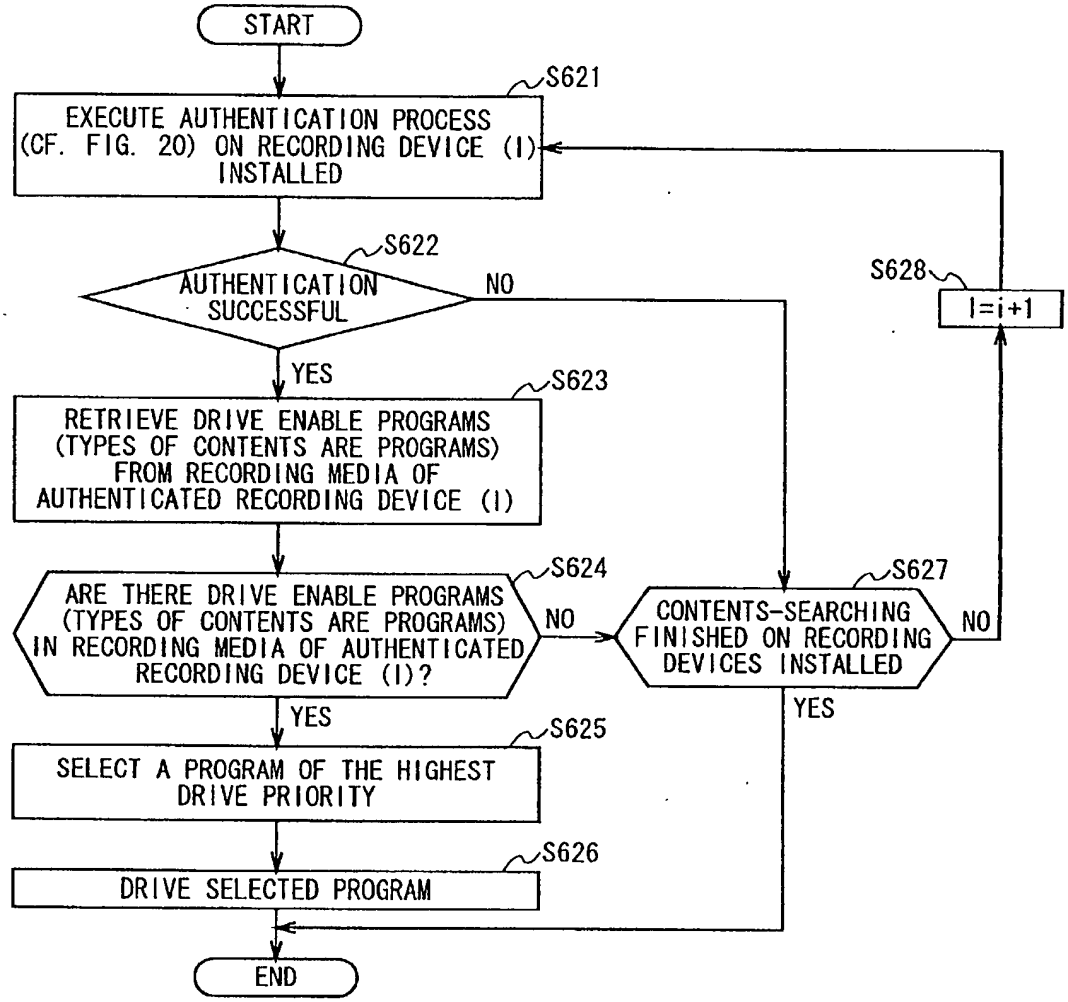

START
S621
EXECUTE AUTHENTICATION PROCESS (CF. FIG. 20) ON RECORDING DEVICE (I) INSTALLED
S622
AUTHENTICATION SUCCESSFUL
NO
YES
S628
I=i+1
S623
RETRIEVE DRIVE ENABLE PROGRAMS (TYPES OF CONTENTS ARE PROGRAMS) FROM RECORDING MEDIA OF AUTHENTICATED RECORDING DEVICE (I)
S624
ARE THERE DRIVE ENABLE PROGRAMS (TYPES OF CONTENTS ARE PROGRAMS) IN RECORDING MEDIA OF AUTHENTICATED RECORDING DEVICE (I)?
NO
S627
CONTENTS-SEARCHING FINISHED ON RECORDING DEVICES INSTALLED
NO
YES
YES
S625
SELECT A PROGRAM OF THE HIGHEST DRIVE PRIORITY
S626
DRIVE SELECTED PROGRAM
END

FIG. 58

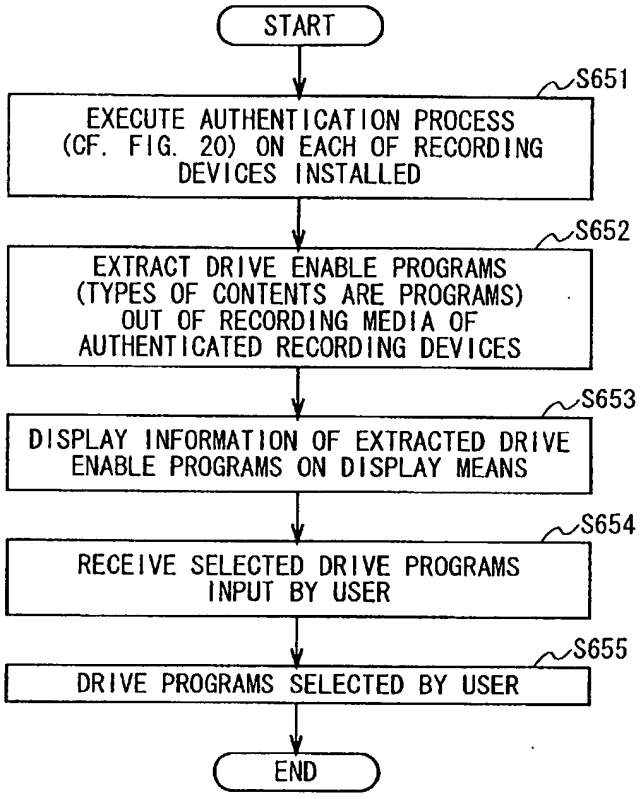


FIG. 59

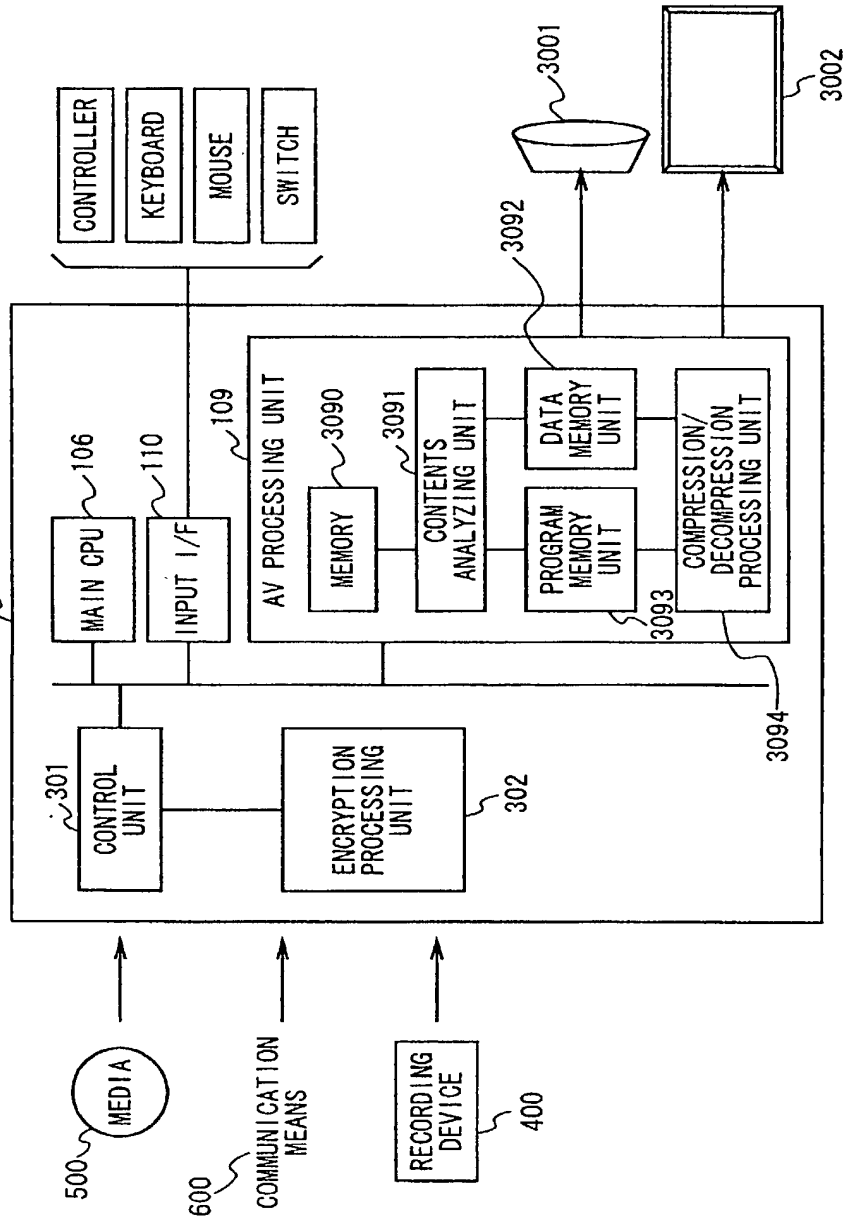

CONTROLLER
KEYBOARD
MOUSE
SWITCH
3001
3002
3092
300
MAIN CPU
106
INPUT I/F
110
109
AV PROCESSING UNIT
MEMORY
3090
CONTENTS ANALYZING UNIT
3091
DATA MEMORY UNIT
PROGRAM MEMORY UNIT
3093
COMPRESSION/ DECOMPRESSION PROCESSING UNIT
3094
301
CONTROL UNIT
ENCRYPTION PROCESSING UNIT
302
500
MEDIA
600
COMMUNICATION MEANS
RECORDING DEVICE
400

FIG. 60

EXAMPLE OF CONTENTS COMPOSITION (1)

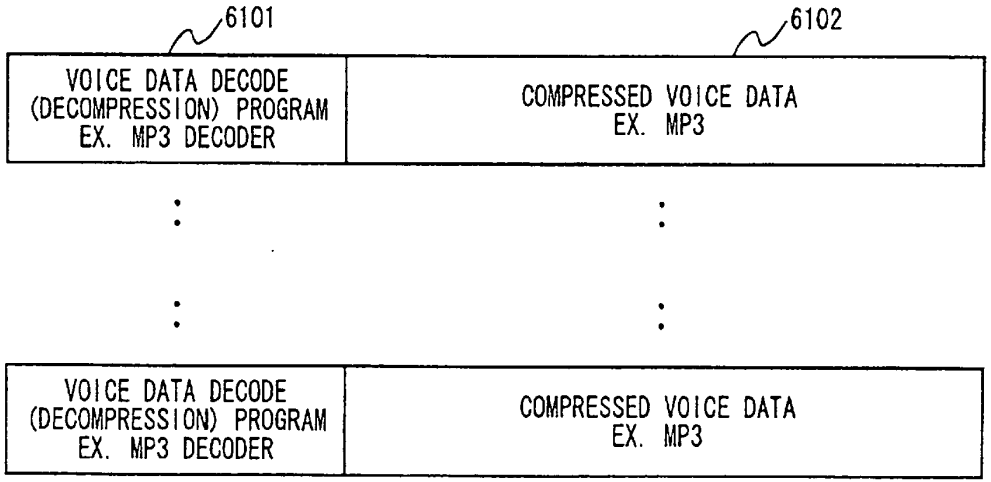


FIG. 61

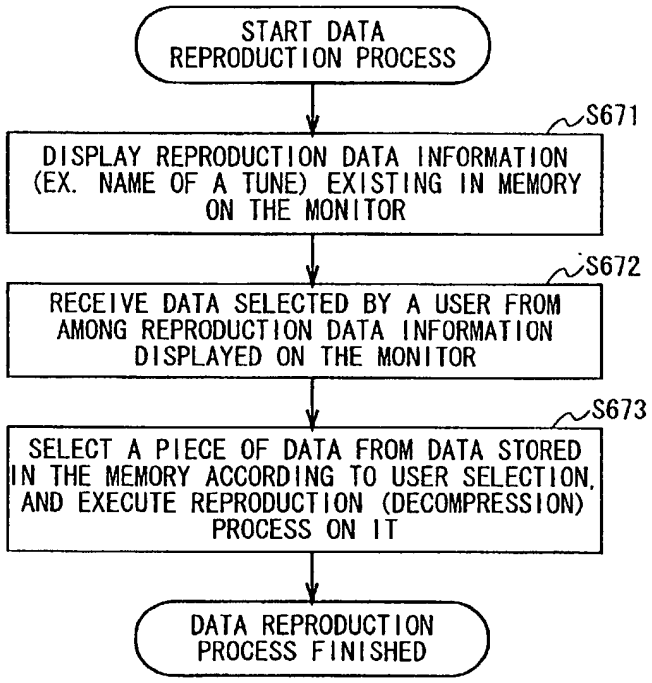

START DATA REPRODUCTION PROCESS
S671
DISPLAY REPRODUCTION DATA INFORMATION (EX. NAME OF A TUNE) EXISTING IN MEMORY ON THE MONITOR
S672
RECEIVE DATA SELECTED BY A USER FROM AMONG REPRODUCTION DATA INFORMATION DISPLAYED ON THE MONITOR
S673
SELECT A PIECE OF DATA FROM DATA STORED IN THE MEMORY ACCORDING TO USER SELECTION, AND EXECUTE REPRODUCTION (DECOMPRESSION) PROCESS ON IT
DATA REPRODUCTION PROCESS FINISHED

FIG. 62

EXAMPLE OF CONTENTS COMPOSITION (2)

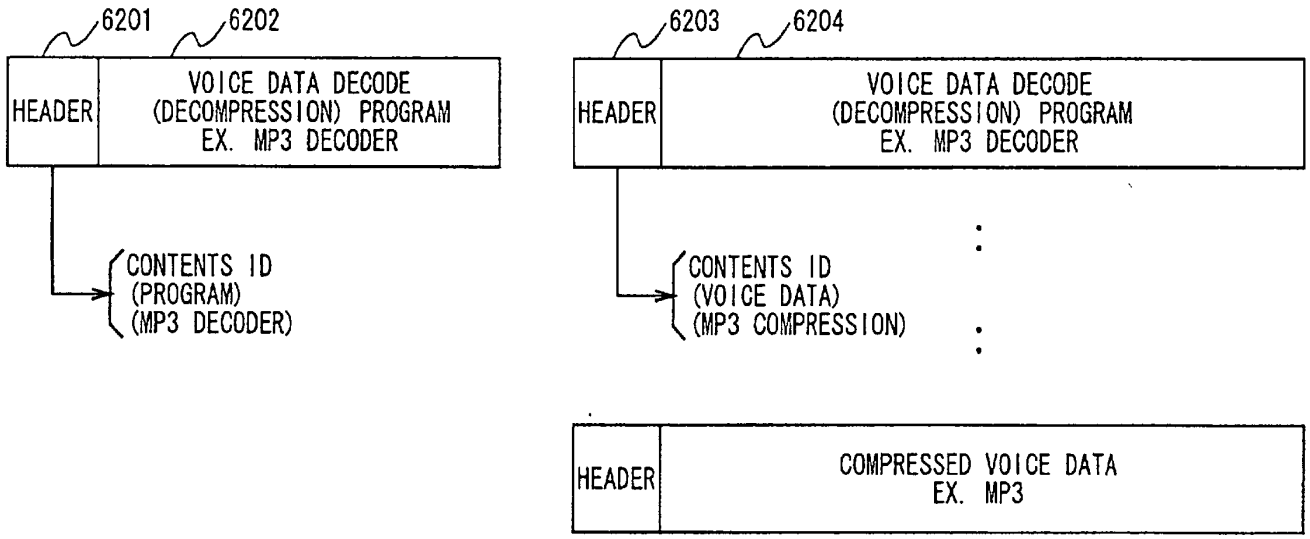


FIG. 63

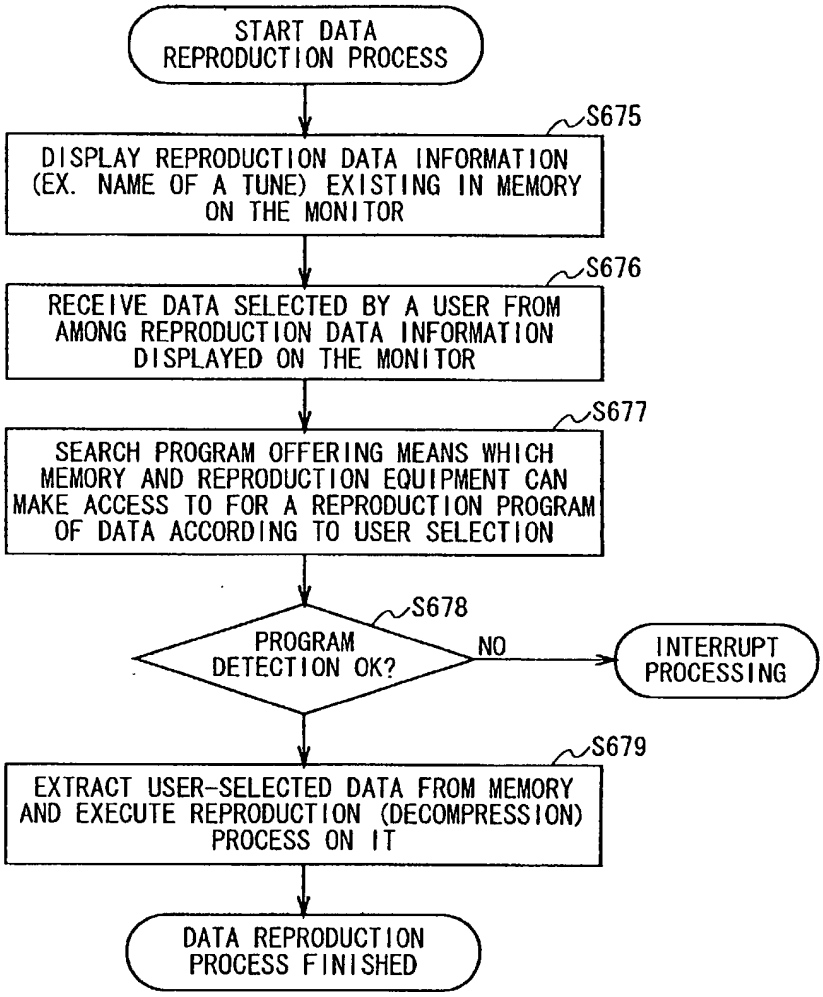

START DATA REPRODUCTION PROCESS
S675
DISPLAY REPRODUCTION DATA INFORMATION (EX. NAME OF A TUNE) EXISTING IN MEMORY ON THE MONITOR
S676
RECEIVE DATA SELECTED BY A USER FROM AMONG REPRODUCTION DATA INFORMATION DISPLAYED ON THE MONITOR
S677
SEARCH PROGRAM OFFERING MEANS WHICH MEMORY AND REPRODUCTION EQUIPMENT CAN MAKE ACCESS TO FOR A REPRODUCTION PROGRAM OF DATA ACCORDING TO USER SELECTION
S678
PROGRAM DETECTION OK?
NO
INTERRUPT PROCESSING
S679
EXTRACT USER-SELECTED DATA FROM MEMORY AND EXECUTE REPRODUCTION (DECOMPRESSION) PROCESS ON IT
DATA REPRODUCTION PROCESS FINISHED

FIG. 64

EXAMPLE OF CONTENTS COMPOSITION (3)

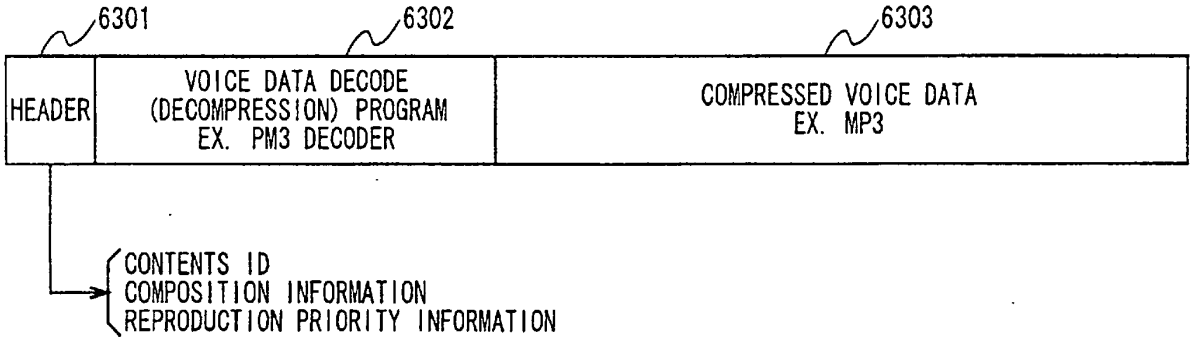


FIG. 65

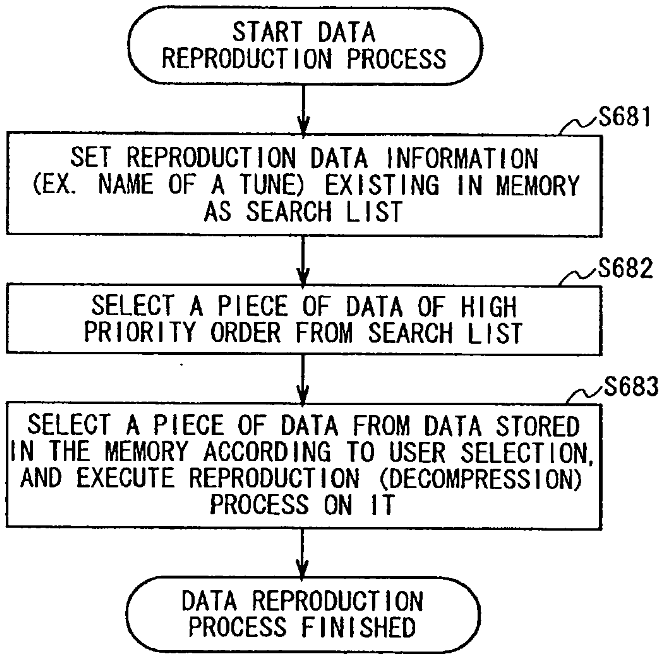


FIG. 66

EXAMPLE OF CONTENTS COMPOSITION (4)

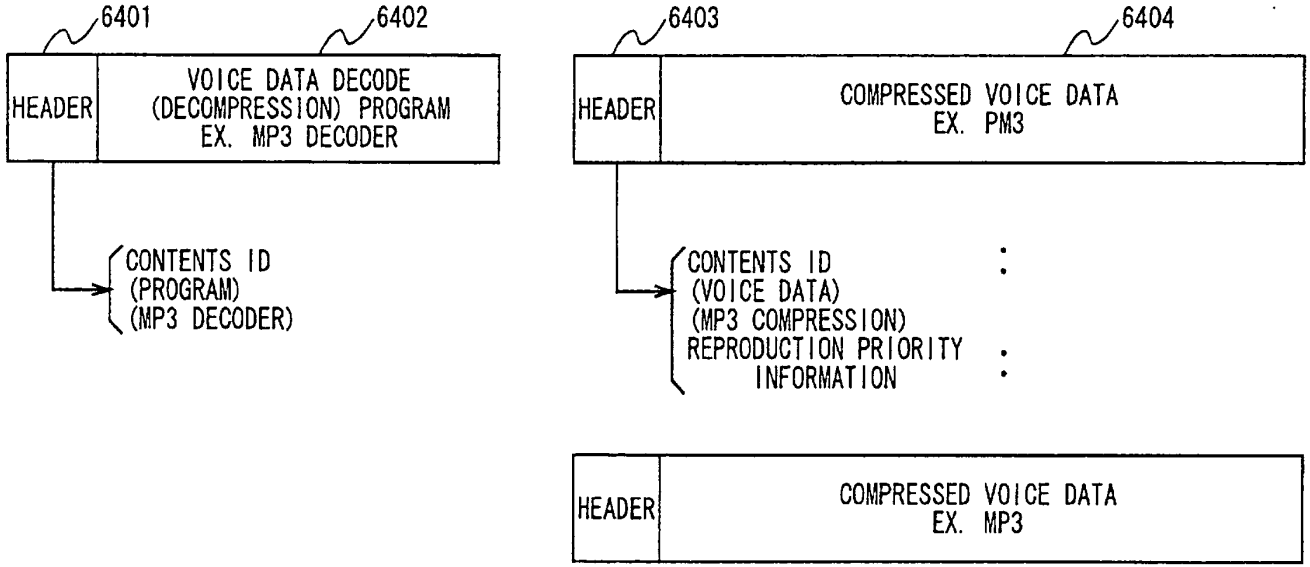


FIG. 67

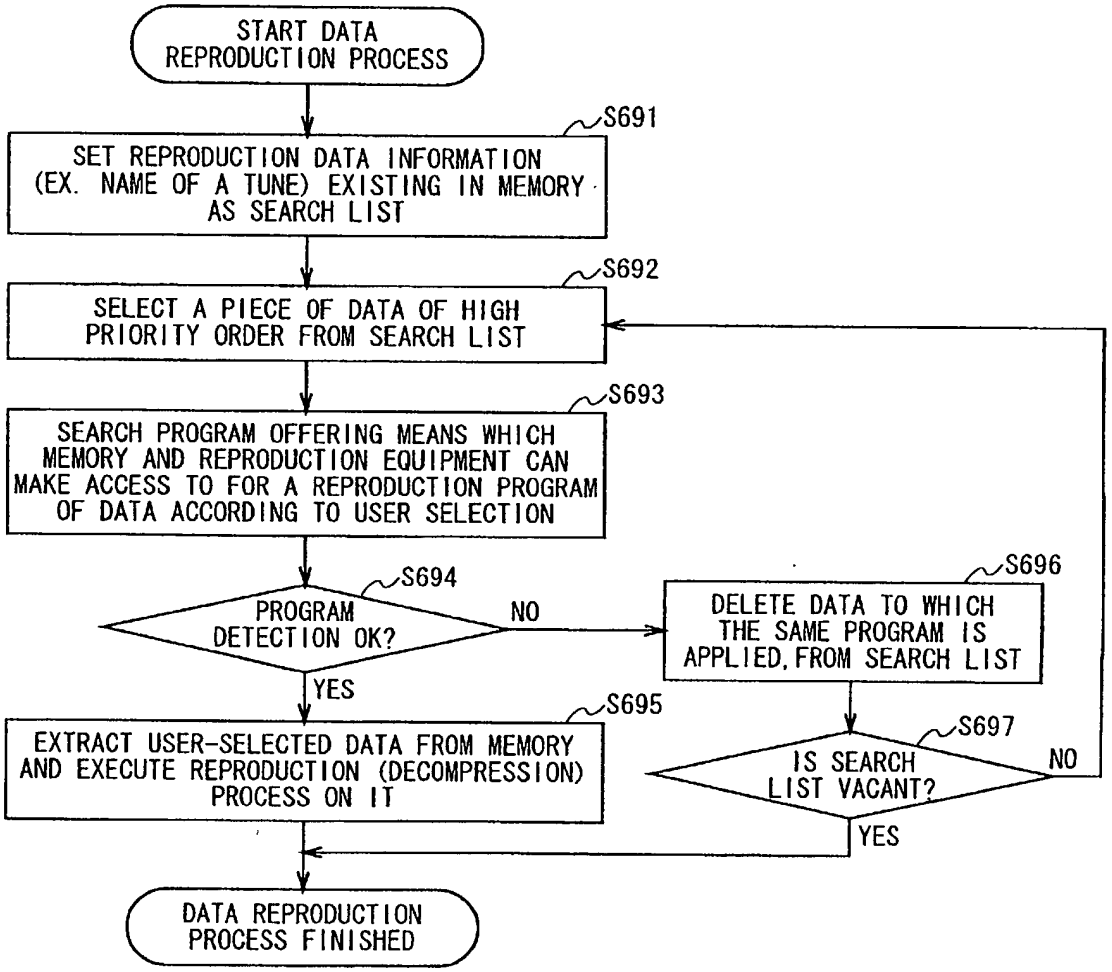
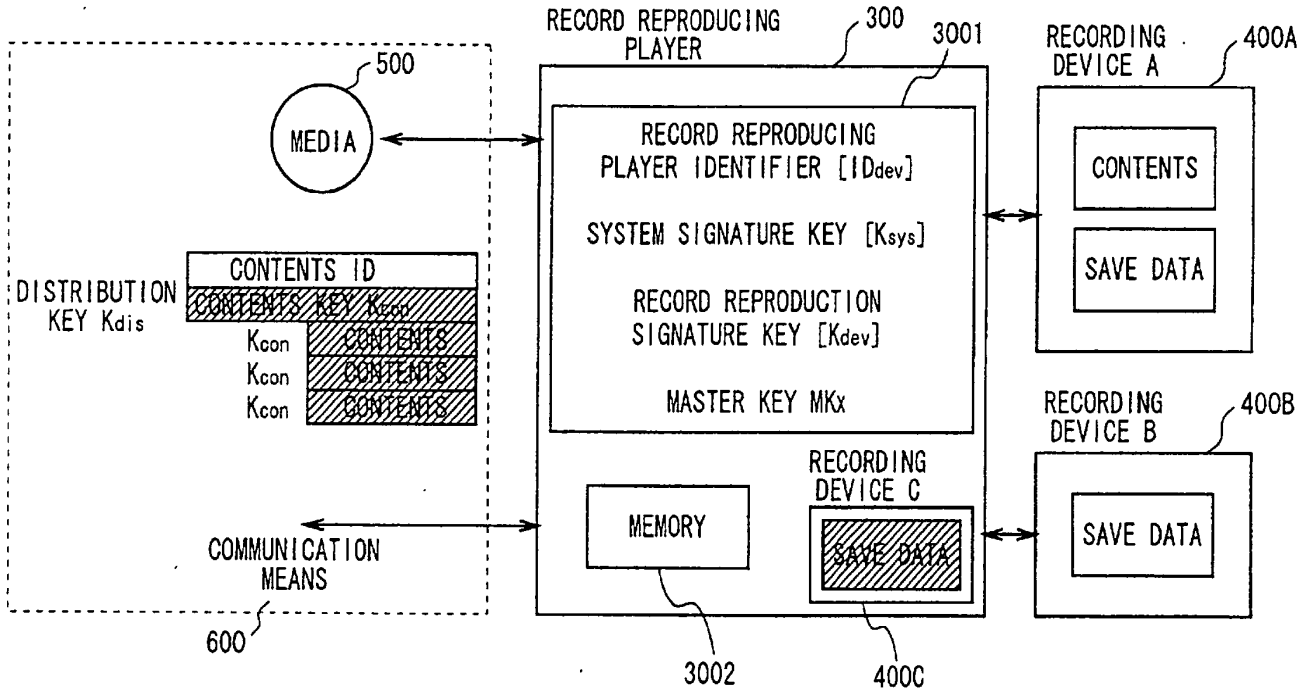

START DATA REPRODUCTION PROCESS
S691
SET REPRODUCTION DATA INFORMATION (EX. NAME OF A TUNE) EXISTING IN MEMORY AS SEARCH LIST
S692
SELECT A PIECE OF DATA OF HIGH PRIORITY ORDER FROM SEARCH LIST
S693
SEARCH PROGRAM OFFERING MEANS WHICH MEMORY AND REPRODUCTION EQUIPMENT CAN MAKE ACCESS TO FOR A REPRODUCTION PROGRAM OF DATA ACCORDING TO USER SELECTION
S694
PROGRAM DETECTION OK?
NO
YES
S696
DELETE DATA TO WHICH THE SAME PROGRAM IS APPLIED, FROM SEARCH LIST
S697
IS SEARCH LIST VACANT?
NO
YES
S695
EXTRACT USER-SELECTED DATA FROM MEMORY AND EXECUTE REPRODUCTION (DECOMPRESSION) PROCESS ON IT
DATA REPRODUCTION PROCESS FINISHED

FIG. 68



SAVE DATA ENCRYPTION KEY:$K_{sav}=K_{con}$
SAVE DATA ENCRYPTION KEY:$K_{sav}=K_{sys}$
SAVE DATA ENCRYPTION KEY:$K_{sav}=K_{dev}$
SAVE DATA ENCRYPTION KEY:K_{sav}=CONTENTS ID, (MKx, CONTENTS ID)
SAVE DATA ENCRYPTION KEY:K_{sav}=RECORD REPRODUCING PLAYER ID (ID_{DEV})
SAVE DATA ENCRYPTION KEY:$K_{sav}=(K_{con} \hat{} K_{dev})$ or DES$(MK_x, K_{con} \hat{} K_{dev})$
SAVE DATA ENCRYPTION KEY:K_{sav}=(CONTENT ID$\hat{}K_{dev}$) or DES(MKx, CONTENT ID$\hat{}K_{dev}$)
SAVE DATA ENCRYPTION KEY:K_{sav}=(KCON$\hat{}$RECORD REPRODUCING PLAYER ID) orDES(MKx, Kcon$\hat{}$RECORD REPRODUCING PLAYER ID)
SAVE DATA ENCRYPTION KEY:K_{sav}=(CONTENTS ID$\hat{}$RECORD REPRODUCING PLAYER ID) orDES
(MKx, CONTENTS ID$\hat{}$RECORD REPRODUCING PLAYER ID)
SAVE DATA ENCRYPTION KEY:K_{sav}=PASSWORD OR DES (MKx, PASSWORD) ETC.

FIG. 69

(1) EXAMPLE OF SAVE DATA STORAGE PROCESS USING CONTENTS INDIVIDUAL KEY, OR SYSTEM SHARED KEY

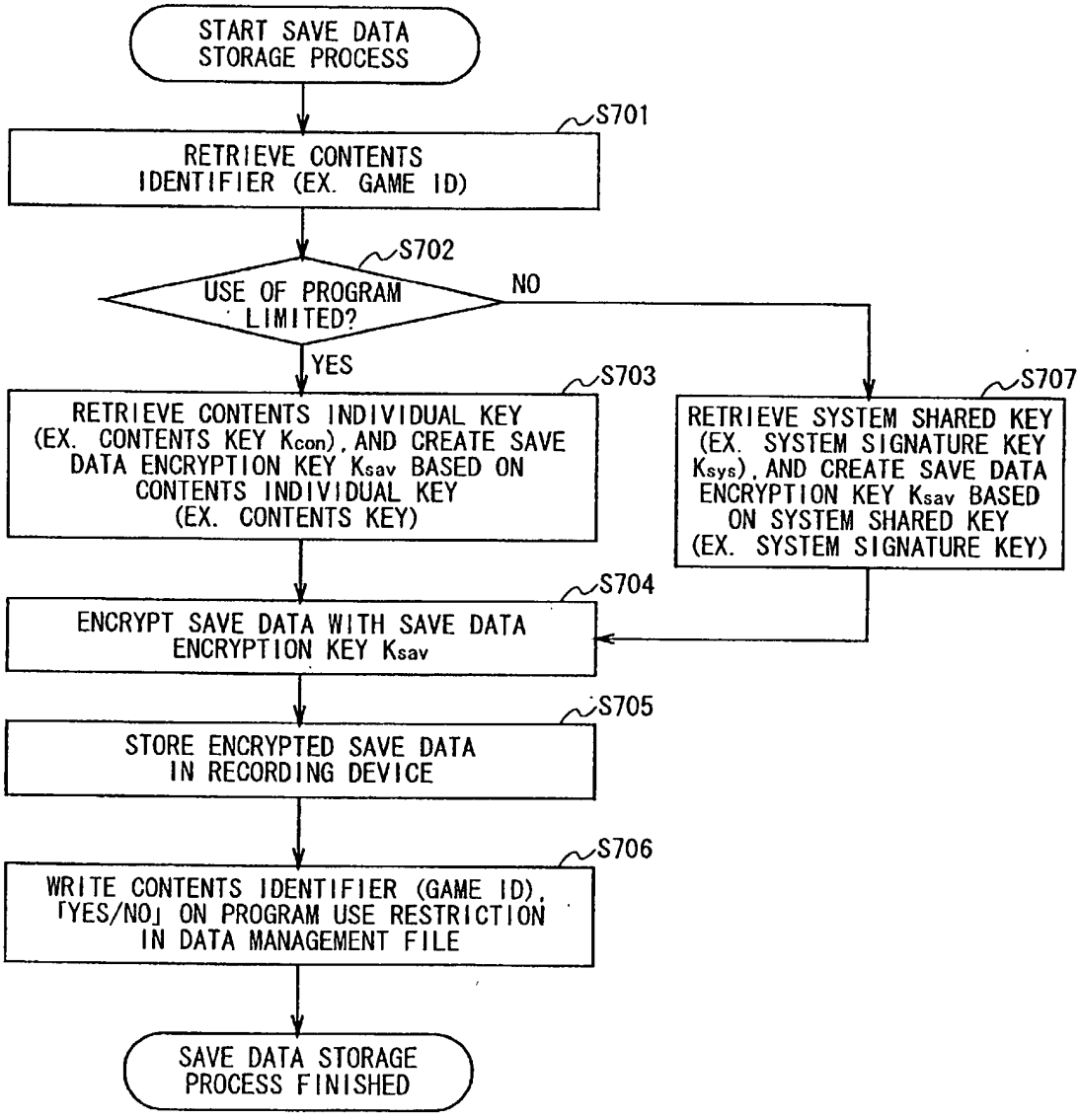


FIG. 70

DATA MANAGEMENT FILE (1)

DATA NO.	CONTENTS IDENTIFIER (GAME ID)	RECORD REPRODUCING PLAYER IDENTIFIER (ID_{dev})	PROGRAM USE RESTRICTION
1	12345678...	56789012...	YES
2	ABCDEF12...	09876543...	YES
3	12245678...	58834762...	NO
:	:	:	:

FIG. 71

(2) EXAMPLE OF SAVE DATA REPRODUCTION PROCESS USING CONTENTS INDIVIDUAL KEY, OR SYSTEM SHARED KEY

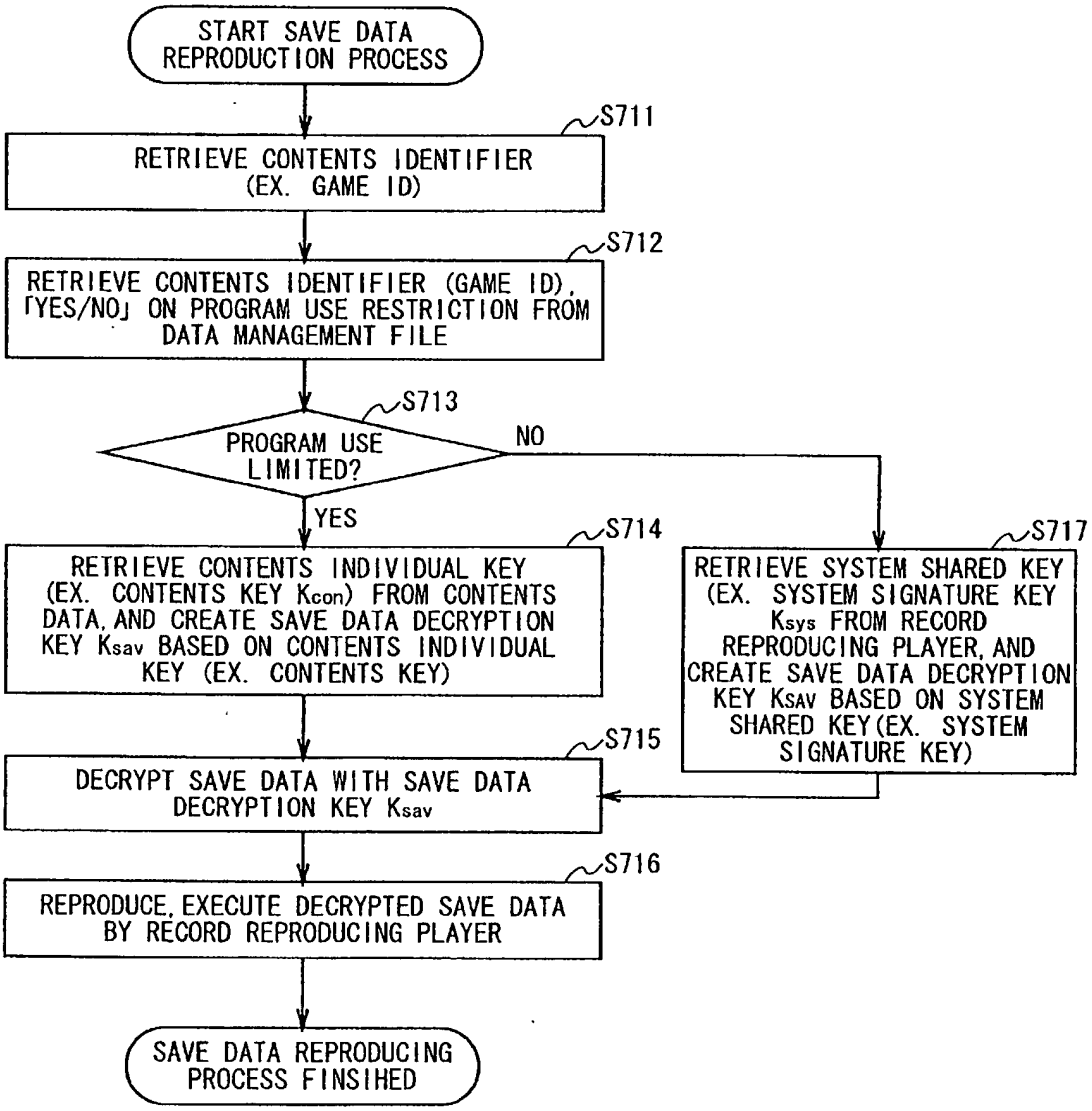


FIG. 72

(3) EXAMPLE OF SAVE DATA STORAGE PROCESS USING CONTENTS ID, OR SYSTEM SHARED KEY

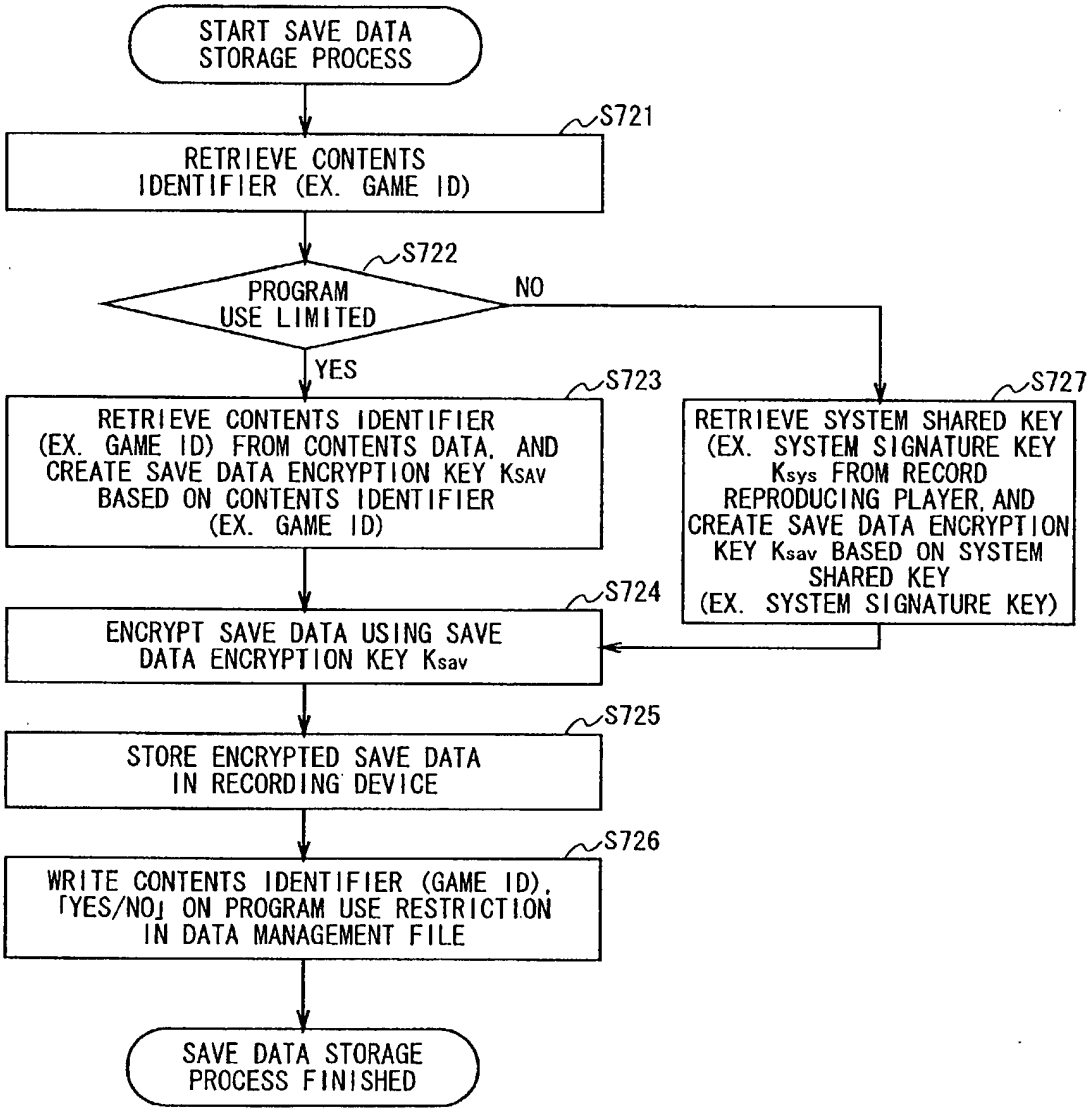


FIG. 73

(4) EXAMPLE OF SAVE DATA REPRODUCTION PROCESS USING CONTENTS ID, OR SYSTEM SHARED KEY

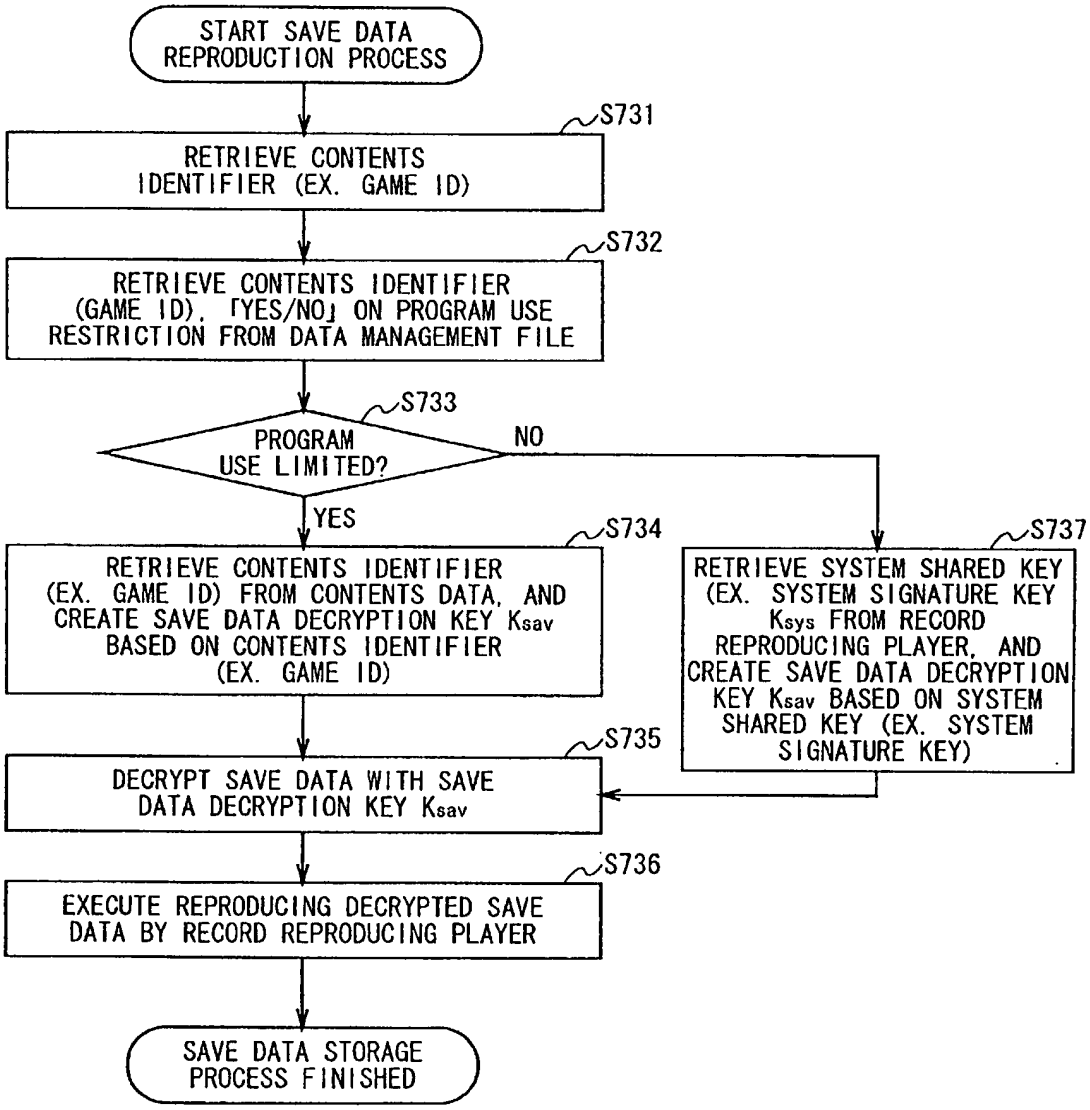


FIG. 74

(5) EXAMPLE OF SAVE DATA STORAGE PROCESS USING RECORD REPRODUCING PLAYER INDIVIDUAL KEY, OR SYSTEM SHARED KEY

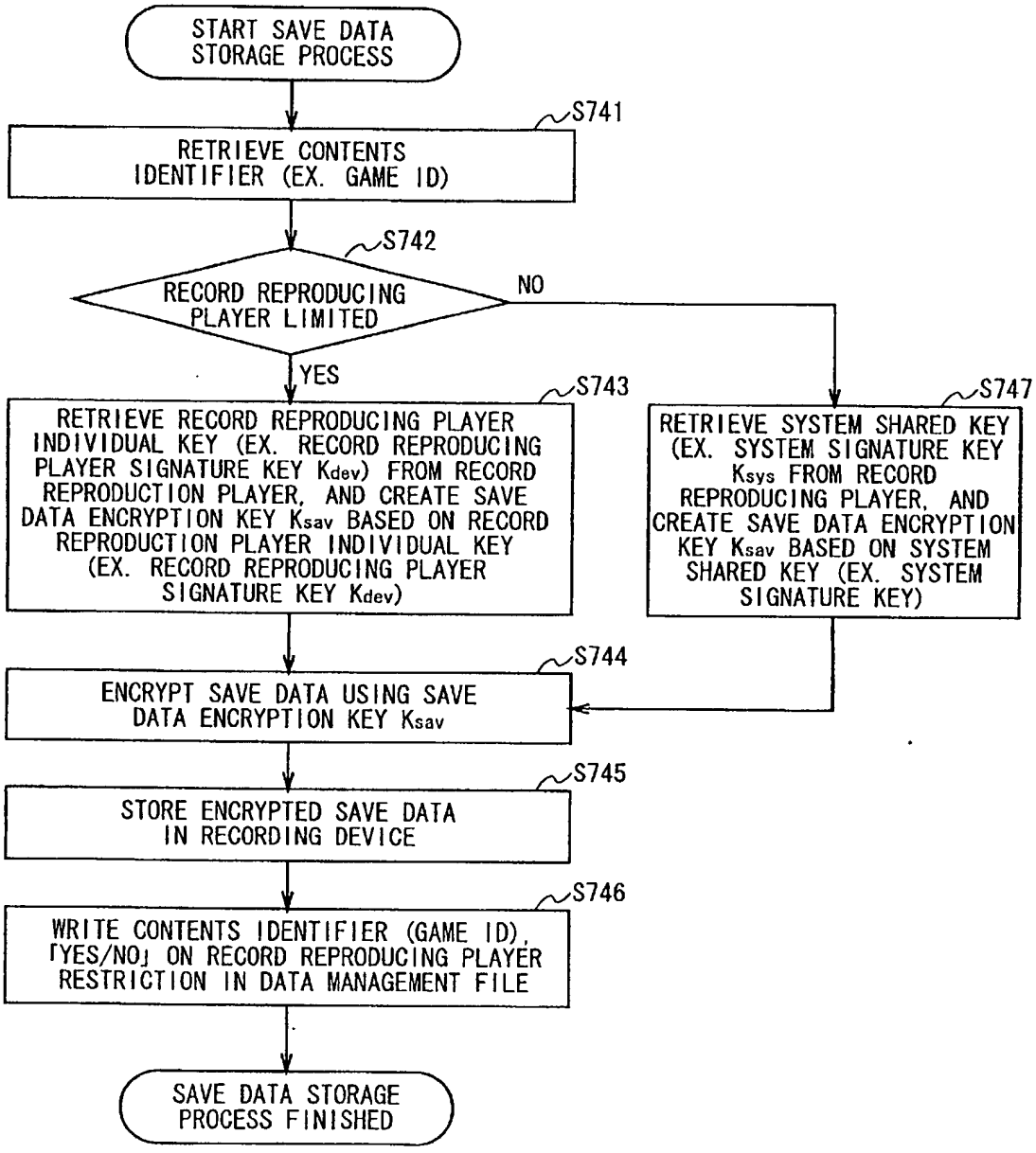


FIG. 75

DATA MANAGEMENT FILE (2)

DATA NO.	CONTENTS IDENTIFIER (GAME ID)	RECORD REPRODUCING PLAYER IDENTIFIER (ID_{dev})	RECORD REPRODUCING PLAYER RESTRICTION
1	12345678...	56789012...	NO
2	ABCDEF12...	09876543...	YES
3	12245678...	58834762...	YES
:	:	:	:

FIG. 76

(6) EXAMPLE OF SAVE DATA REPRODUCTION PROCESS USING RECORD REPRODUCING PLAYER INDIVIDUAL KEY, OR SYSTEM SHARED KEY

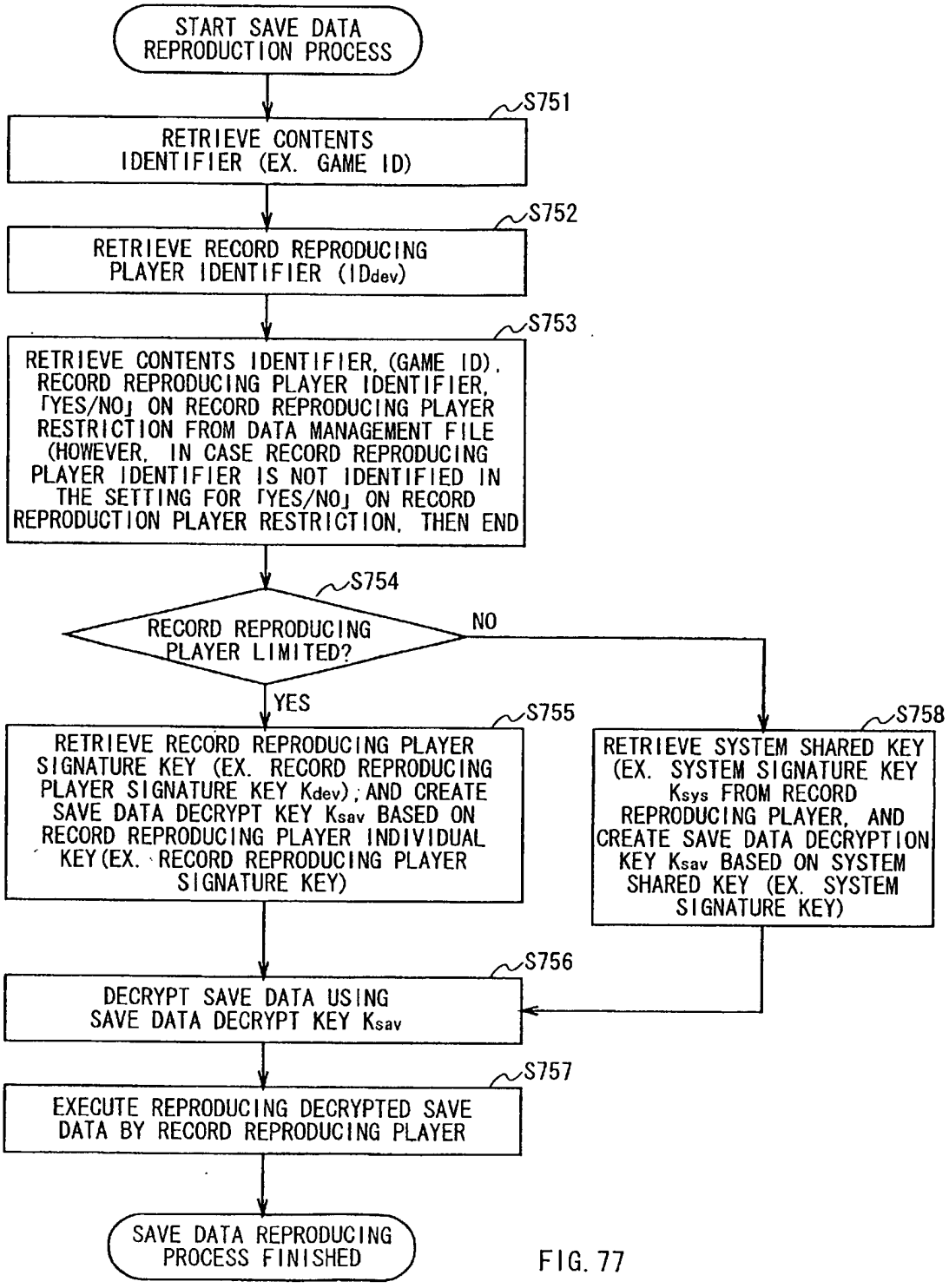


FIG. 77

(7) EXAMPLE OF SAVE DATA STORAGE PROCESS USING RECORD REPRODUCING PLAYER IDENTIFIER, OR SYSTEM SHARED KEY

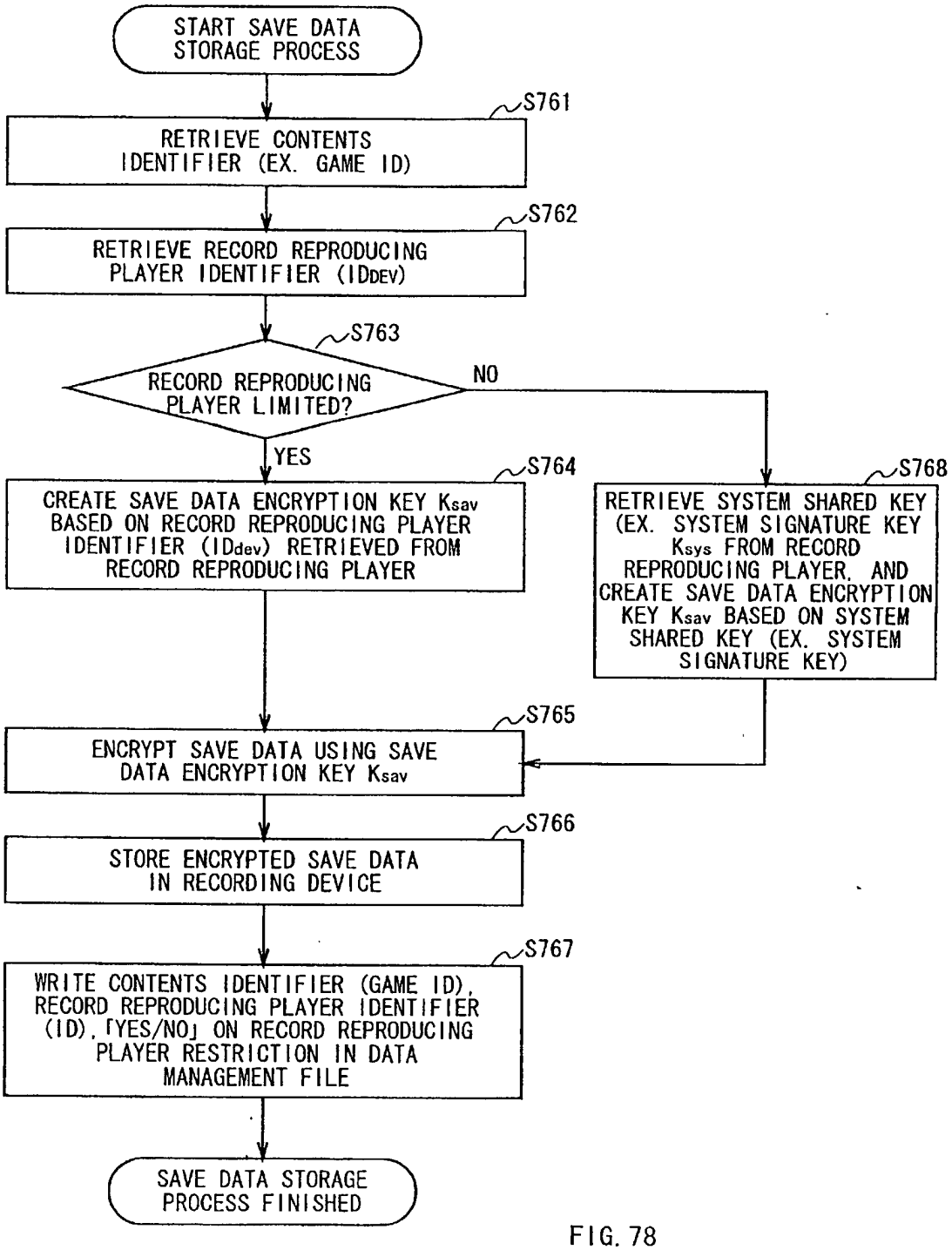


FIG. 78

(8) EXAMPLE OF SAVE DATA REPRODUCTION PROCESS USING RECORD REPRODUCING PLAYER IDENTIFIER, OR SYSTEM SHARED KEY

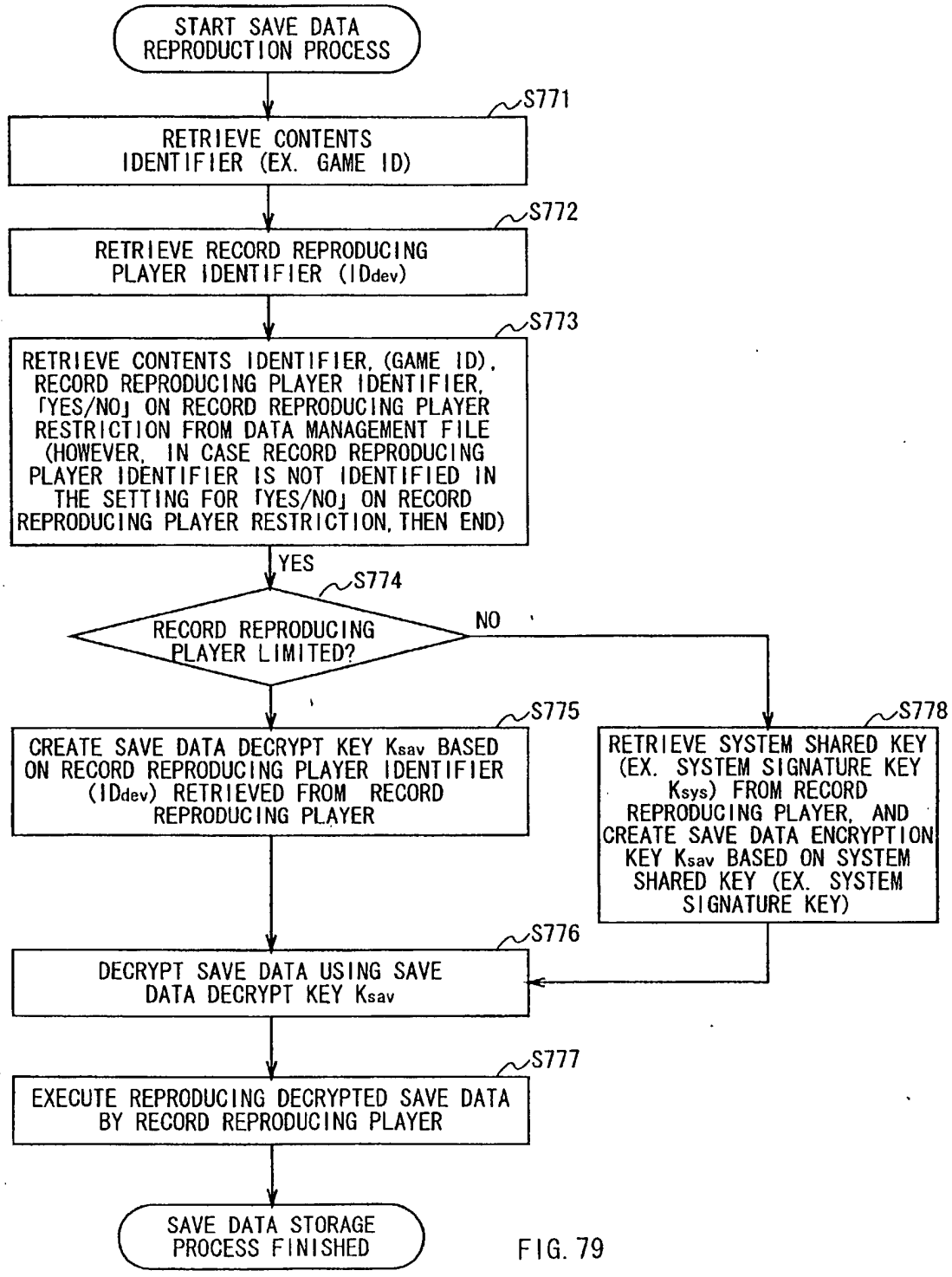


FIG. 79

(9) EXAMPLE OF SAVE DATA STORAGE PROCESS USING CONTENTS INDIVIDUAL KEY, RECORD REPRODUCING PLAYER INDIVIDUAL KEY, OR SYSTEM SHARED KEY

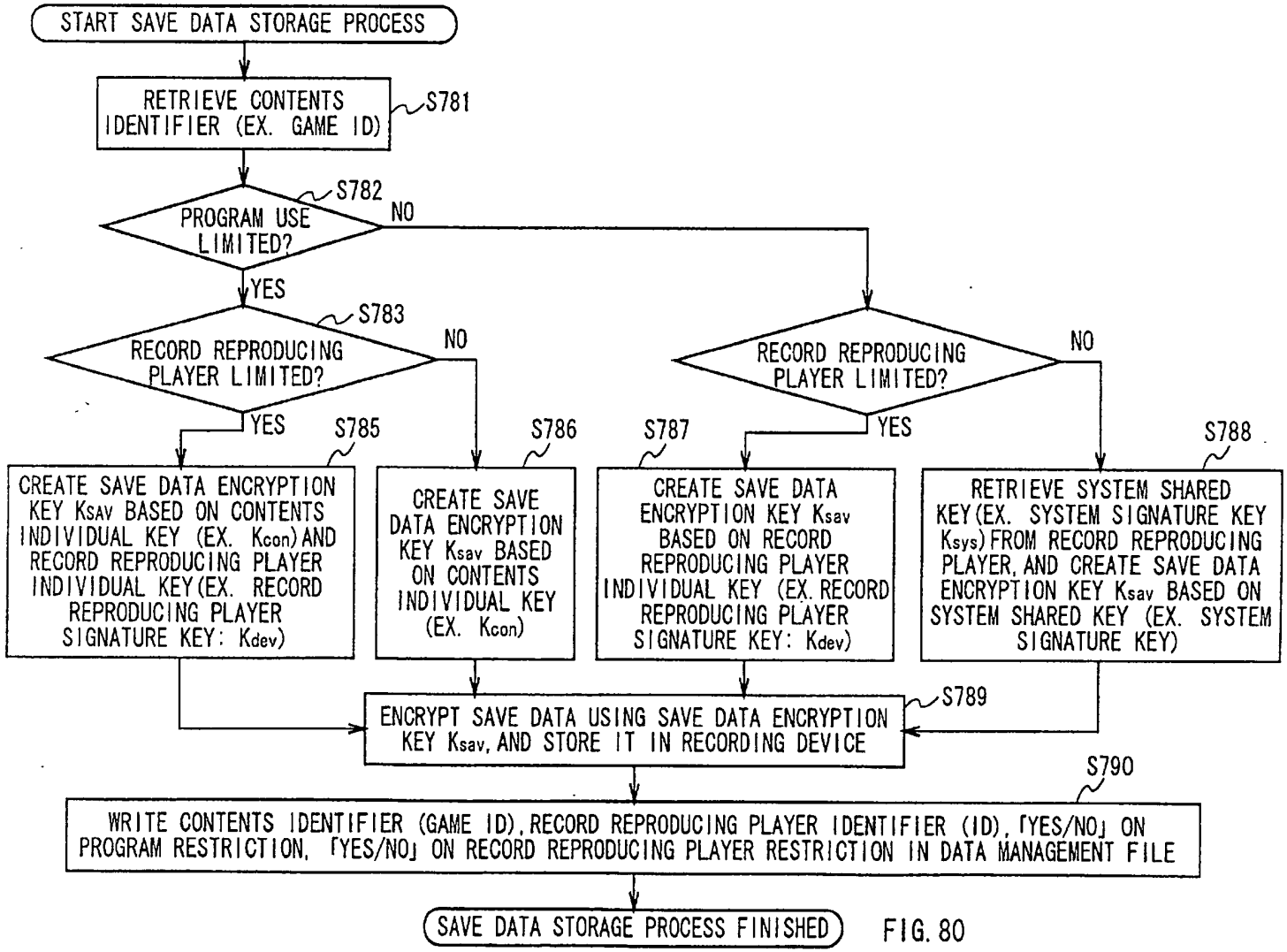


FIG. 80

DATA MANAGEMENT FILE (3)

DATA NO.	CONTENTS IDENTIFIER (GAME ID)	RECORD REPRODUCING PLAYER IDENTIFIER (ID_{dev})	PROGRAM USE RESTRICTION	RECORD REPRODUCING PLAYER RESTRICTION
1	123455678...	56789012...	YES	NO
2	ABCDEF12...	09876543...	YES	YES
3	1122457678	58834762...	NO	YES
⋮	⋮	⋮	⋮	⋮

FIG. 81

(10) EXAMPLE OF SAVE DATA REPRODUCTION PROCESS USING CONTENT UNIQUE KEY, RECORDING AND REPRODUCING DEVICE UNIQUE KEY, OR SYSTEM COMMON KEY

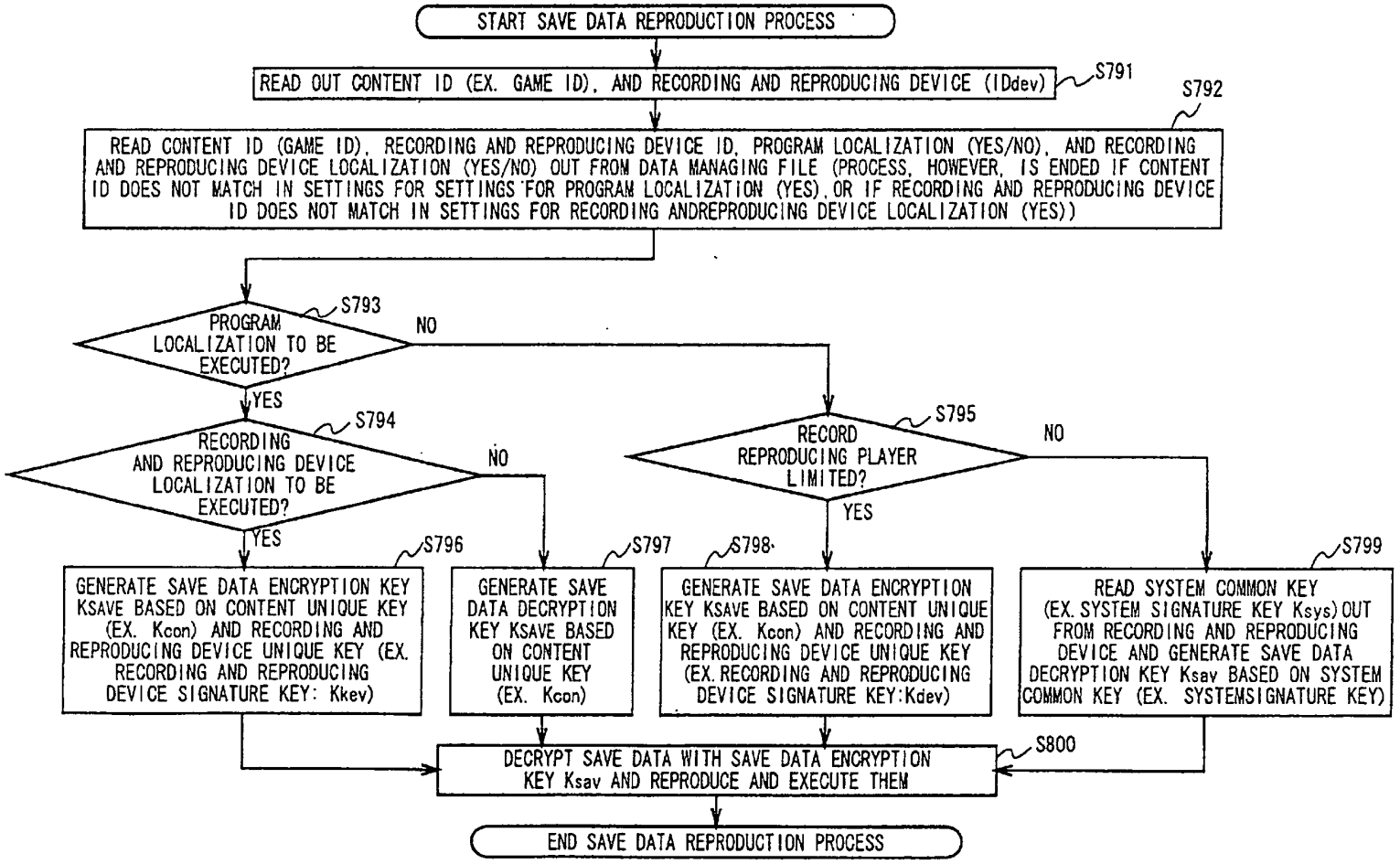


FIG. 82

(11) EXAMPLE OF SAVE DATA STORAGE PROCESS USING USER PASSWORD, OR SYSTEM SHARED KEY

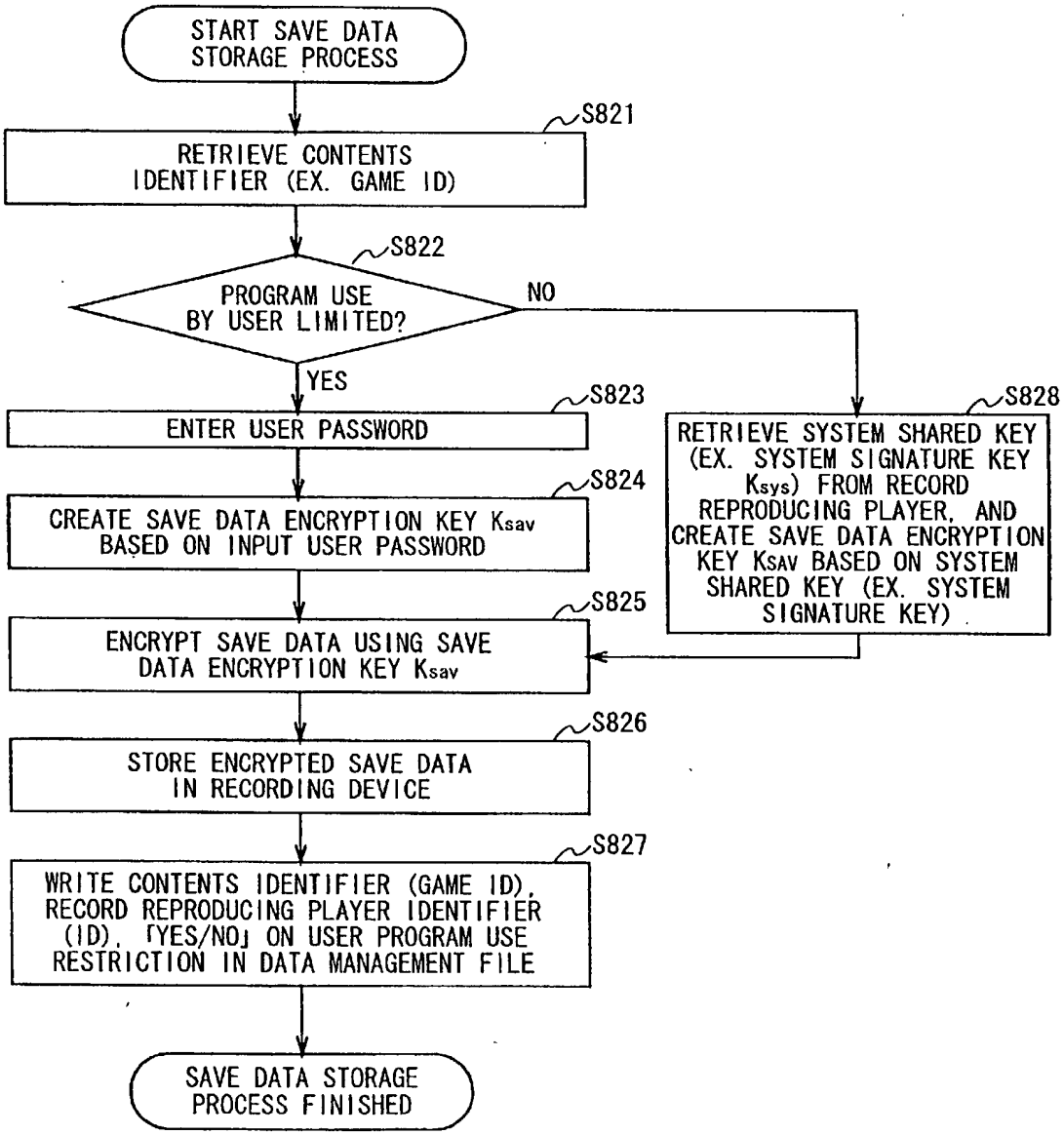


FIG. 83

DATA MANAGEMENT FILE (4)

DATA NO.	CONTENTS IDENTIFIER (GAME ID)	RECORD REPRODUCING PLAYER IDENTIFIER (ID_{dev})	USER PROGRAM USE RESTRICTION
1	123455678...	56789012...	YES
2	ABCDEF12...	09876543...	YES
3	1122457678	58834762...	NO
⋮	⋮	⋮	⋮

FIG. 84

(12) EXAMPLE OF SAVE DATA REPRODUCTION PROCESS USING USER PASSWORD, OR SYSTEM SHARED KEY

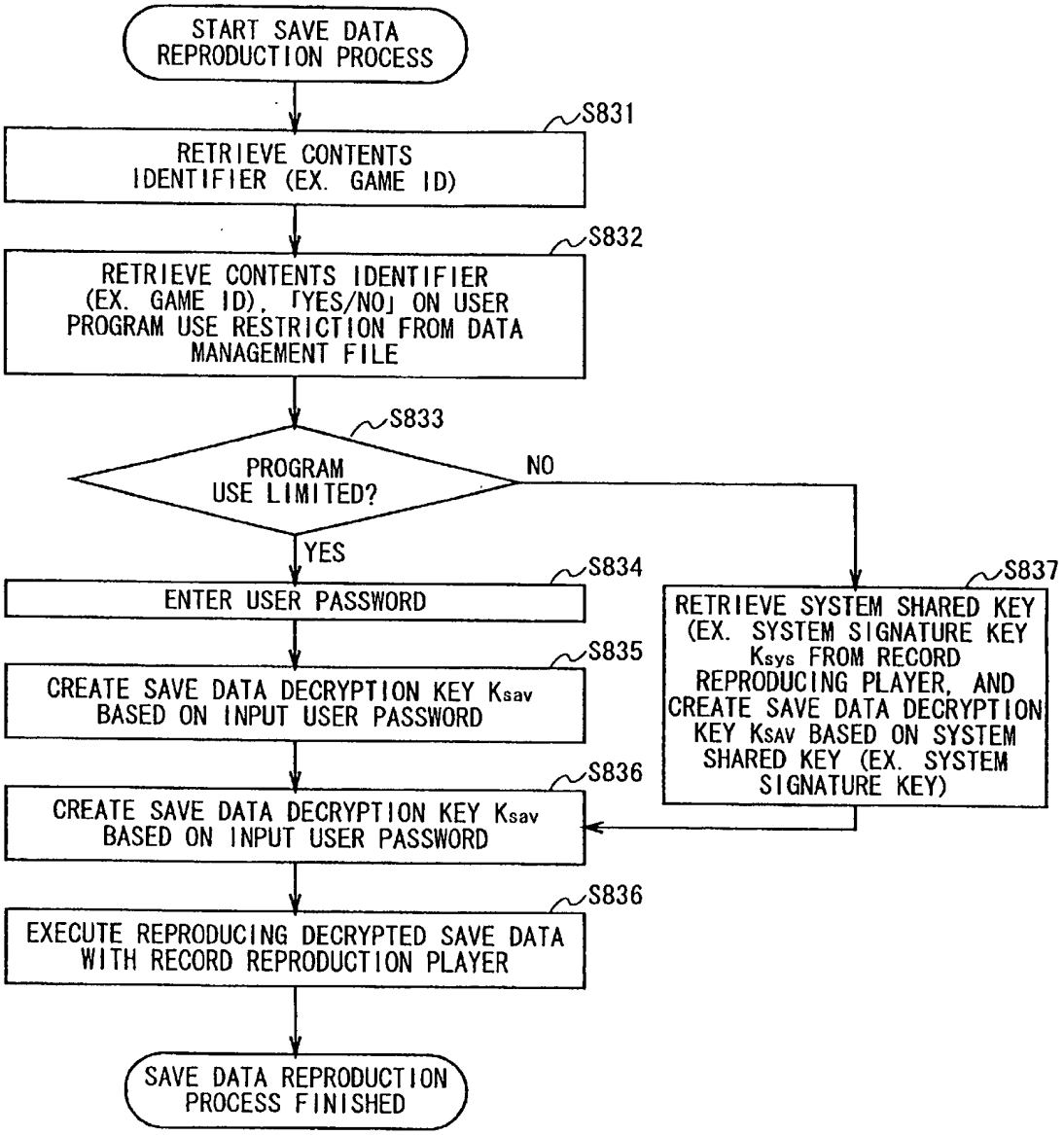


FIG. 85

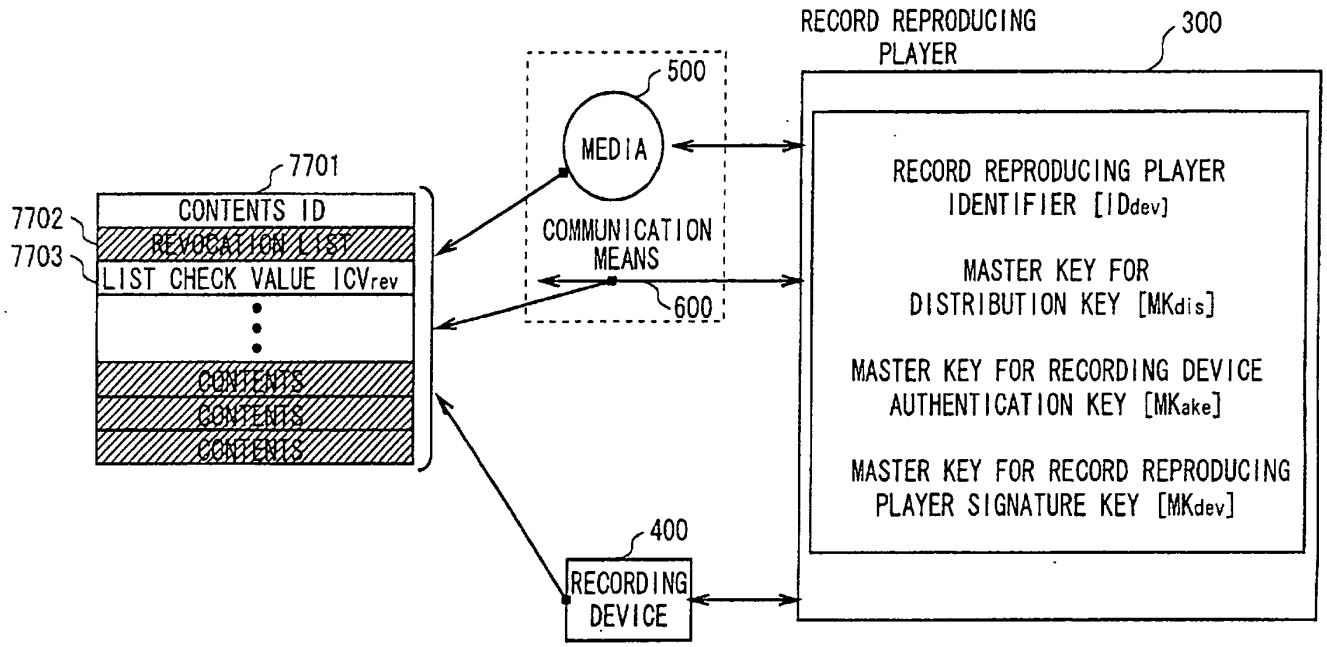

RECORD REPRODUCING PLAYER
300
500
MEDIA
7701
7702
7703
CONTENTS ID
REVOCATION LIST
LIST CHECK VALUE ICVrev
CONTENTS
CONTENTS
CONTENTS
COMMUNICATION MEANS
600
RECORD REPRODUCING PLAYER IDENTIFIER [IDdev]
MASTER KEY FOR DISTRIBUTION KEY [MKdis]
MASTER KEY FOR RECORDING DEVICE AUTHENTICATION KEY [MKake]
MASTER KEY FOR RECORD REPRODUCING PLAYER SIGNATURE KEY [MKdev]
400
RECORDING DEVICE

FIG. 86

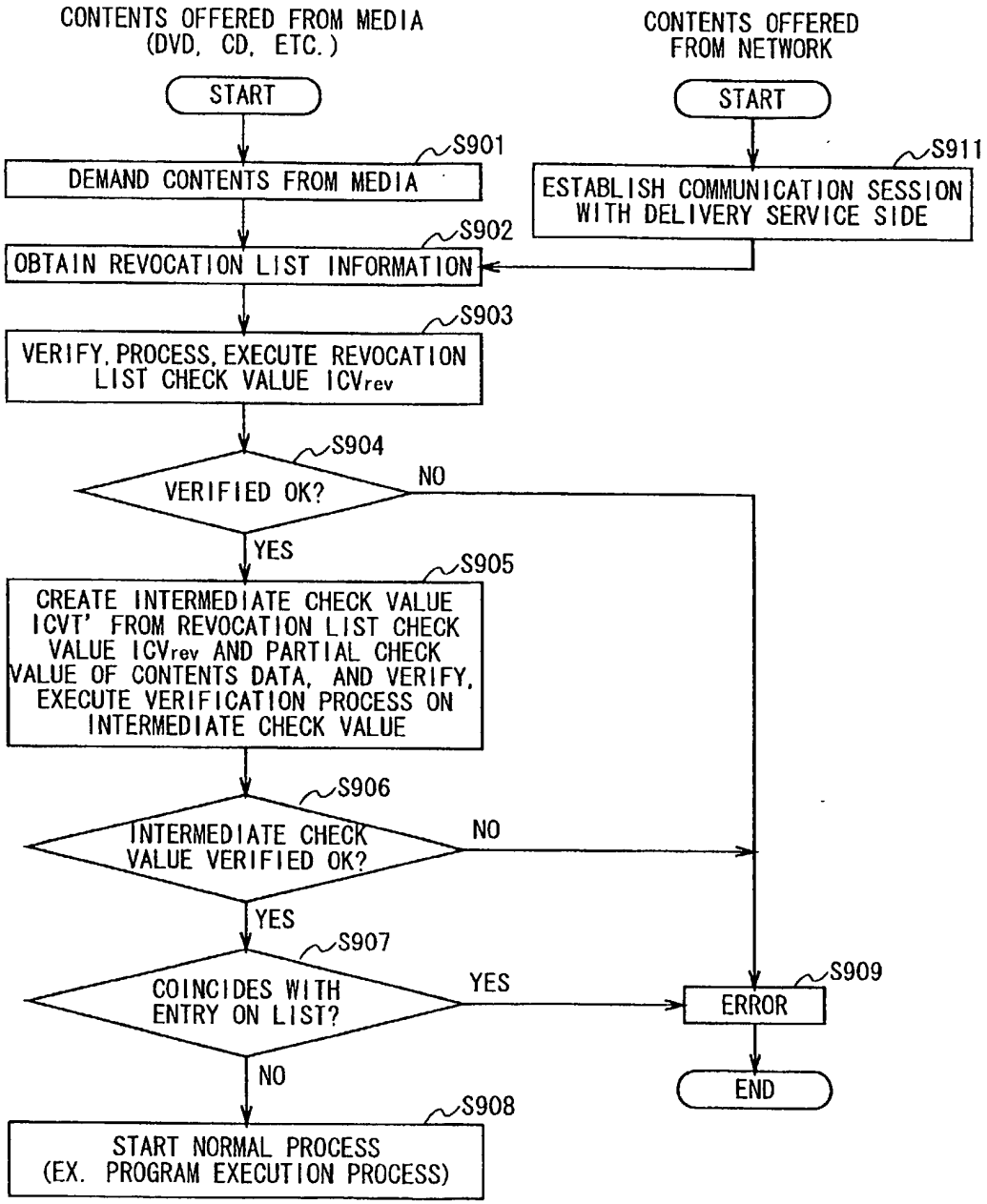

CONTENTS OFFERED FROM MEDIA (DVD, CD, ETC.)
START
S901
DEMAND CONTENTS FROM MEDIA
S902
OBTAIN REVOCATION LIST INFORMATION
S903
VERIFY, PROCESS, EXECUTE REVOCATION LIST CHECK VALUE ICVrev
S904
VERIFIED OK?
NO
YES
S905
CREATE INTERMEDIATE CHECK VALUE ICVT' FROM REVOCATION LIST CHECK VALUE ICVrev AND PARTIAL CHECK VALUE OF CONTENTS DATA, AND VERIFY, EXECUTE VERIFICATION PROCESS ON INTERMEDIATE CHECK VALUE
S906
INTERMEDIATE CHECK VALUE VERIFIED OK?
NO
YES
S907
COINCIDES WITH ENTRY ON LIST?
YES
NO
S908
START NORMAL PROCESS (EX. PROGRAM EXECUTION PROCESS)
CONTENTS OFFERED FROM NETWORK
START
S911
ESTABLISH COMMUNICATION SESSION WITH DELIVERY SERVICE SIDE
S909
ERROR
END

FIG. 87

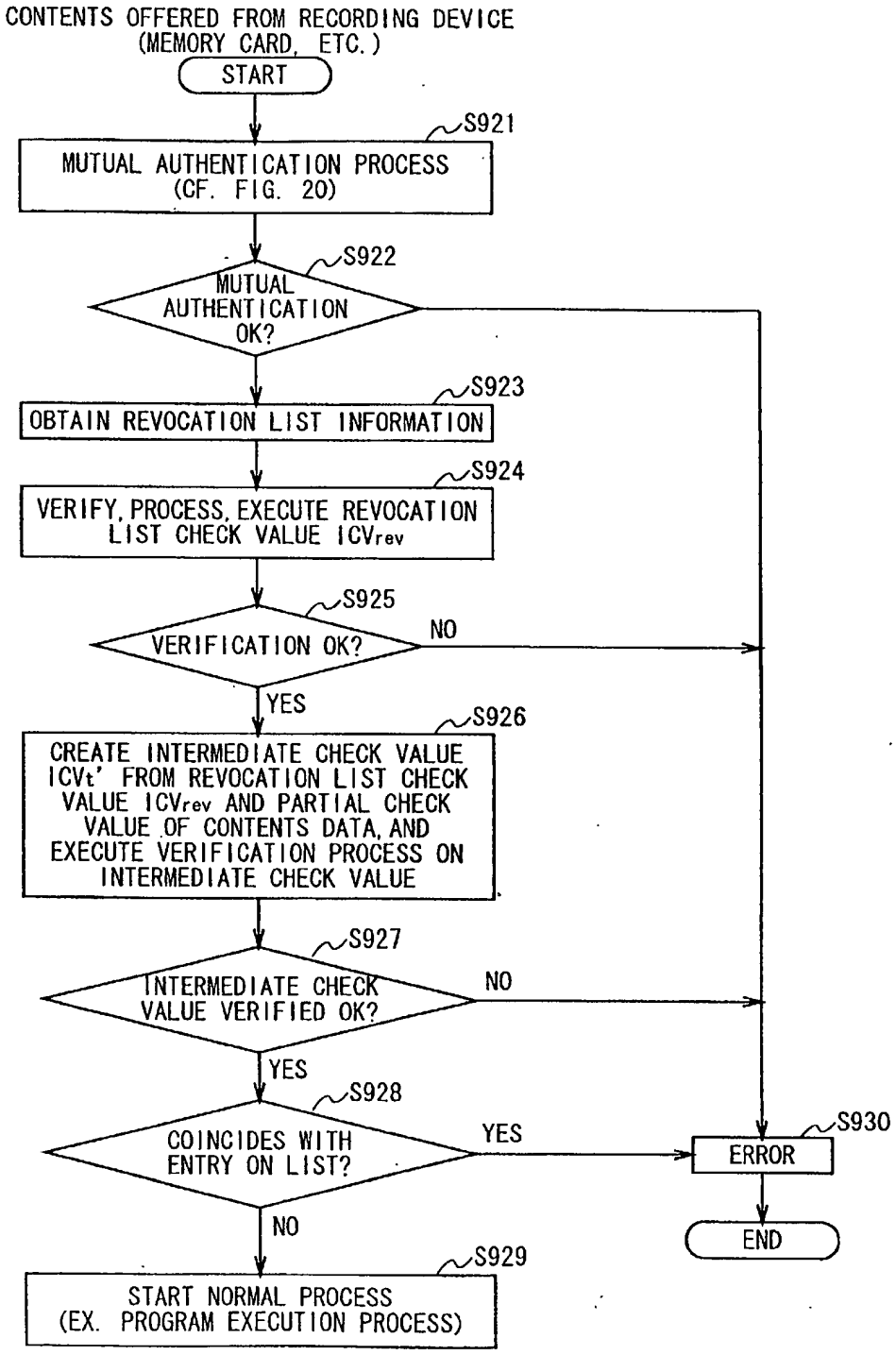

CONTENTS OFFERED FROM RECORDING DEVICE (MEMORY CARD, ETC.)
START
S921
MUTUAL AUTHENTICATION PROCESS (CF. FIG. 20)
S922
MUTUAL AUTHENTICATION OK?
S923
OBTAIN REVOCATION LIST INFORMATION
S924
VERIFY, PROCESS, EXECUTE REVOCATION LIST CHECK VALUE ICVrev
S925
VERIFICATION OK?
NO
YES
S926
CREATE INTERMEDIATE CHECK VALUE ICVt' FROM REVOCATION LIST CHECK VALUE ICVrev AND PARTIAL CHECK VALUE OF CONTENTS DATA, AND EXECUTE VERIFICATION PROCESS ON INTERMEDIATE CHECK VALUE
S927
INTERMEDIATE CHECK VALUE VERIFIED OK?
NO
YES
S928
COINCIDES WITH ENTRY ON LIST?
YES
S930
ERROR
END
NO
S929
START NORMAL PROCESS (EX. PROGRAM EXECUTION PROCESS)

FIG. 88

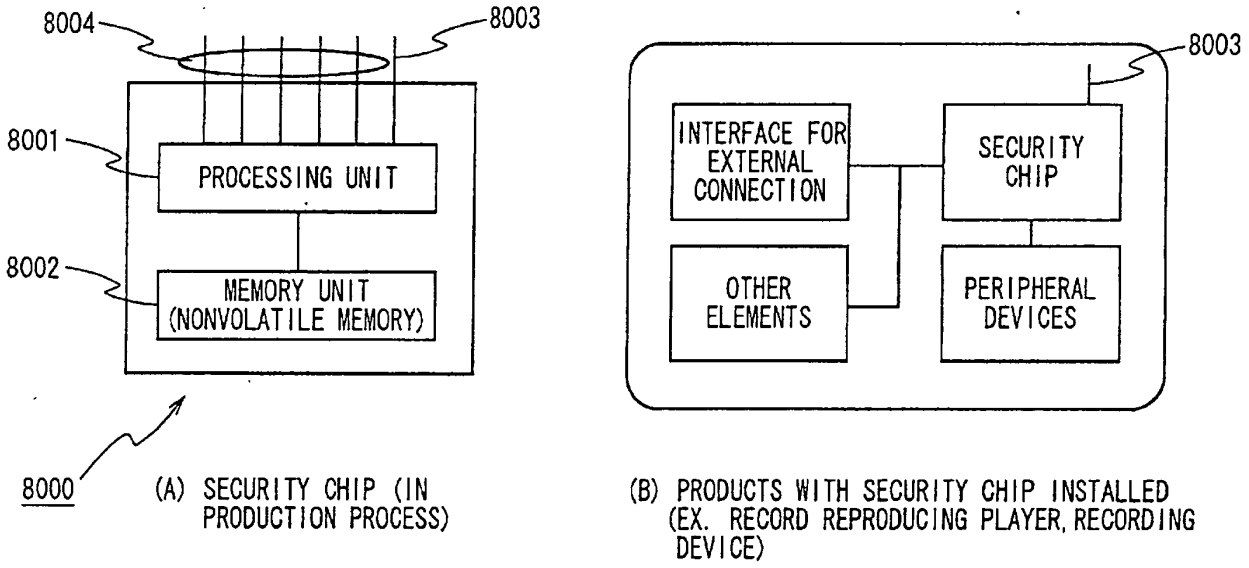


FIG. 89

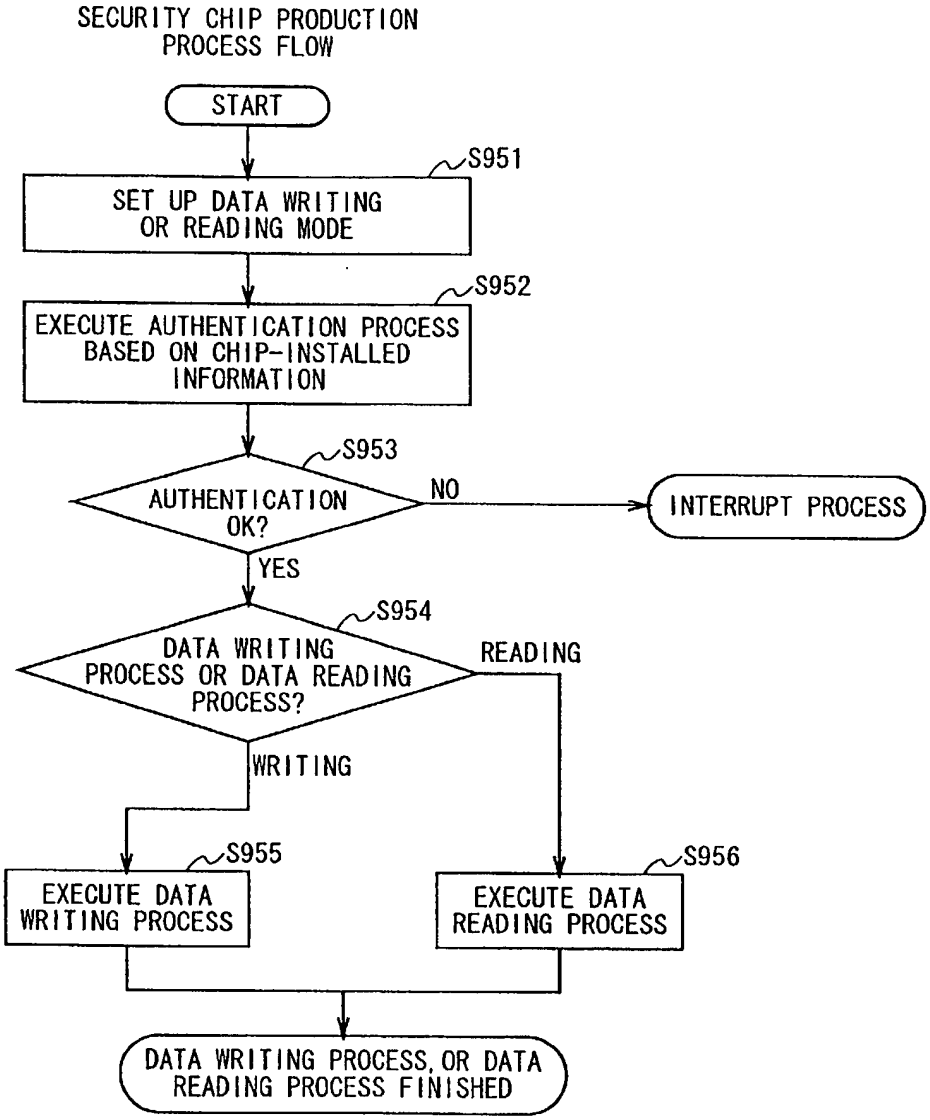
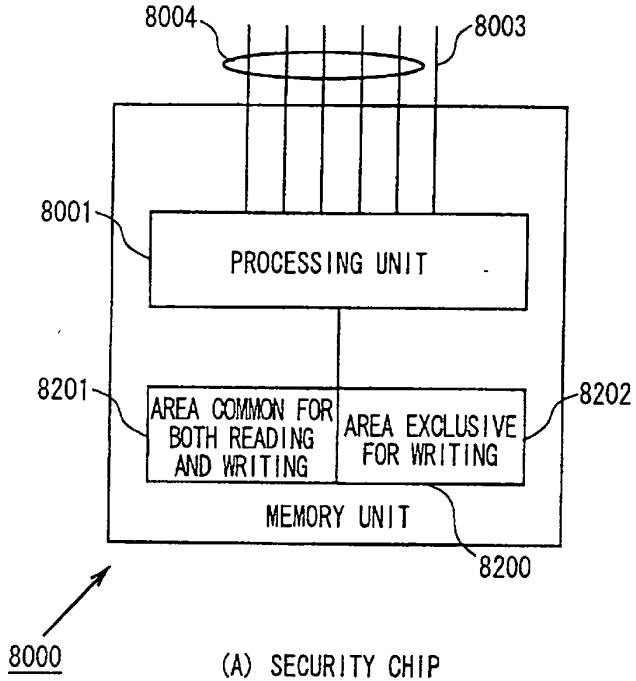
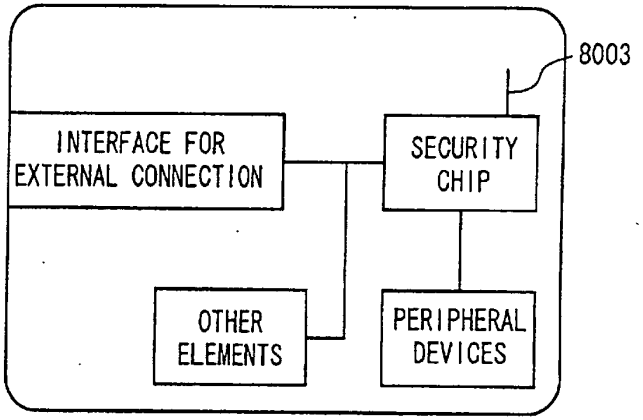

SECURITY CHIP PRODUCTION PROCESS FLOW
START
S951
SET UP DATA WRITING OR READING MODE
S952
EXECUTE AUTHENTICATION PROCESS BASED ON CHIP-INSTALLED INFORMATION
S953
AUTHENTICATION OK?
NO
INTERRUPT PROCESS
YES
S954
DATA WRITING PROCESS OR DATA READING PROCESS?
READING
WRITING
S955
EXECUTE DATA WRITING PROCESS
S956
EXECUTE DATA READING PROCESS
DATA WRITING PROCESS, OR DATA READING PROCESS FINISHED

FIG. 90



(A) SECURITY CHIP
(IN PRODUCTION PROCESS)



(B) PRODUCTS WITH SECURITY CHIP INSTALLED
(EX. RECORD REPRODUCING PLAYER, RECORDING DEVICE)

FIG. 91

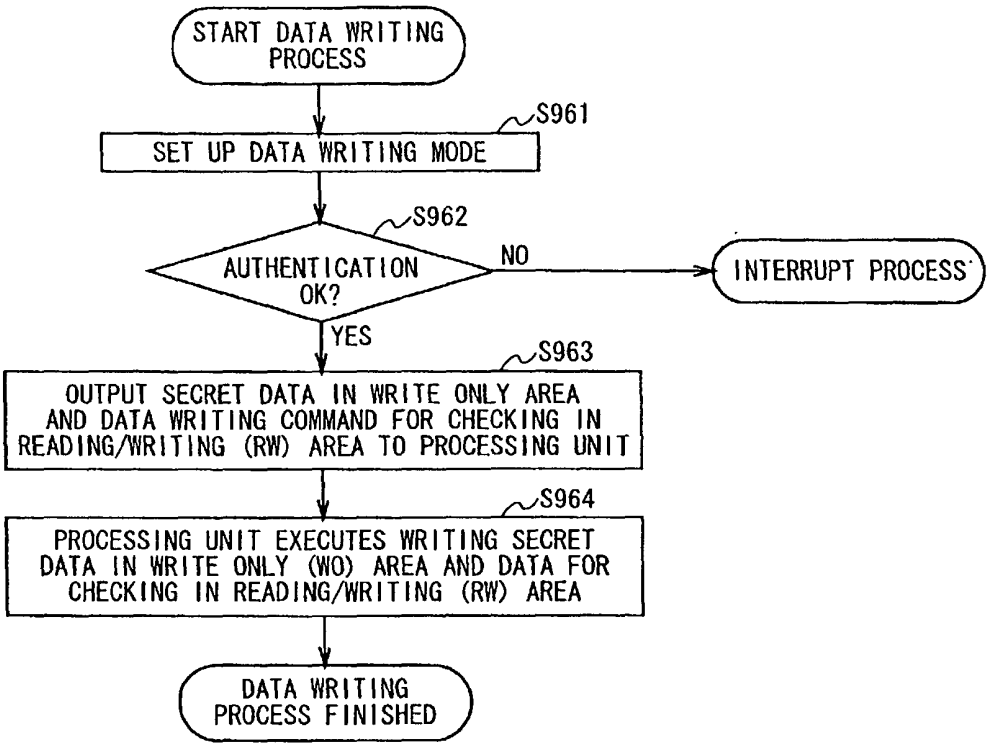

START DATA WRITING PROCESS
S961
SET UP DATA WRITING MODE
S962
AUTHENTICATION OK?
NO
INTERRUPT PROCESS
YES
S963
OUTPUT SECRET DATA IN WRITE ONLY AREA AND DATA WRITING COMMAND FOR CHECKING IN READING/WRITING (RW) AREA TO PROCESSING UNIT
S964
PROCESSING UNIT EXECUTES WRITING SECRET DATA IN WRITE ONLY (WO) AREA AND DATA FOR CHECKING IN READING/WRITING (RW) AREA
DATA WRITING PROCESS FINISHED

FIG. 92

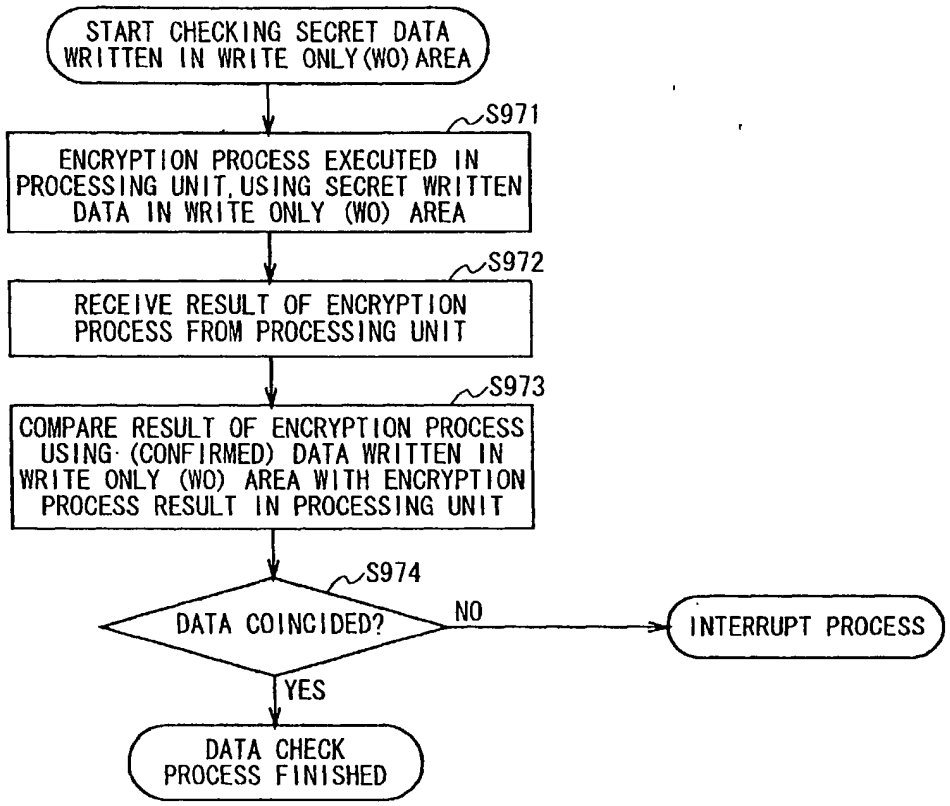


FIG. 93

Explanation of Reference Numerals

106 - - main CPU, 107 - - RAM, 108 - - ROM, 109 - - AV processing unit, 110 - - input processing unit, 111 - - PIO, 112 - - SIO, 300 - - record reproduction player, 301 - - control unit, 302 - - encryption processing unit, 303 - - recording device controller, 304 - - read unit, 305 - - communication unit, 306 - - control unit, 307 - - internal memory, 308 - - encryption/decryption unit, 400 - - recording device, 401 - - encryption processing unit, 402 - - external memory, 403 - - control unit, 404 - - communication unit, 405 - - internal memory, 406 - - encryption/decryption unit, 407 -- external memory control unit, 500 - - media, 600 - - communication means, 2101, 2102, 2103 - - record reproduction player, 2104, 2105, 2106 - - recording device, 2901 - - command numbers management unit, 2902 - - command register, 2903, 2904 - - authentication flag, 3001 - - speaker, 3002 - - monitor, 3090 - - memory, 3091 - - contents analyzing unit, 3092 - - data memory unit, 3093 - program memory unit, 3094 - - compression/ decompression processing unit, 7701 - - contents data, 7702 - revocation list, 7703 - - list check value, 8000 - - security chip, 8001 - - processing unit, 8002 - - memory unit, 8003 - - mode signal line, 8004 - - command signal line, 8201 - - read/write area, 8201 - write only area